

Merchant Transaction Server 104

118, 120, 122 = optional

Figure 1

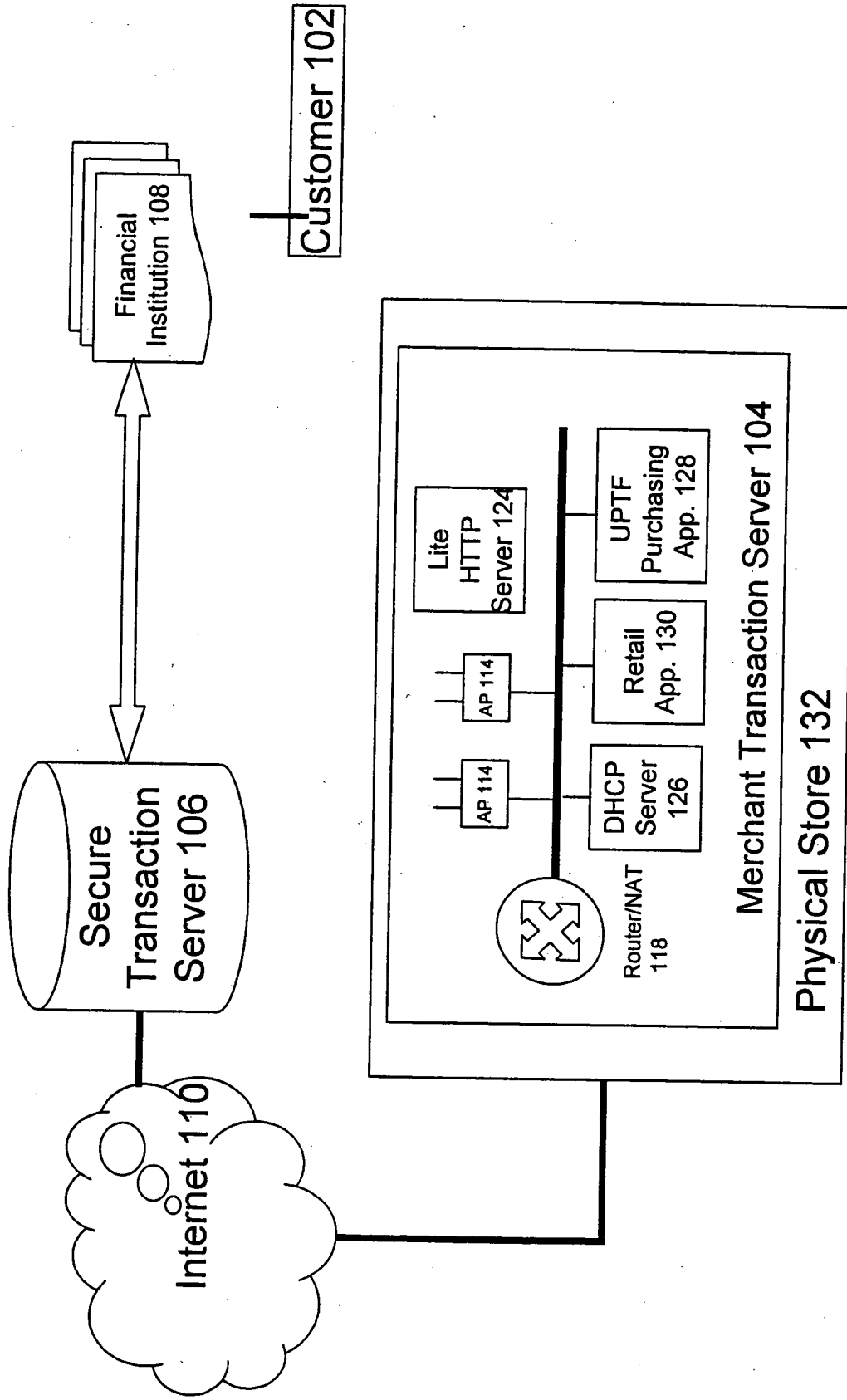


Figure 2

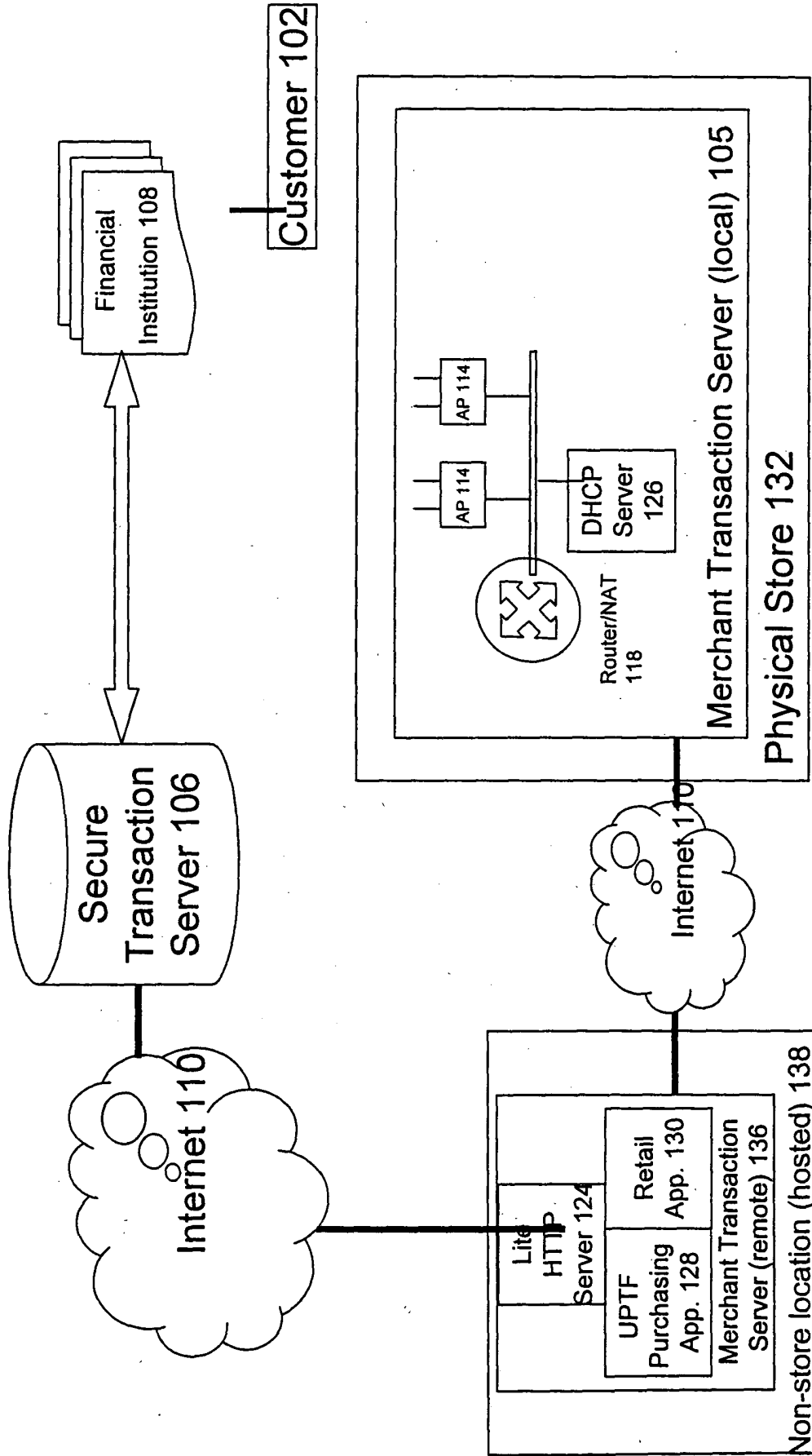


Figure 3

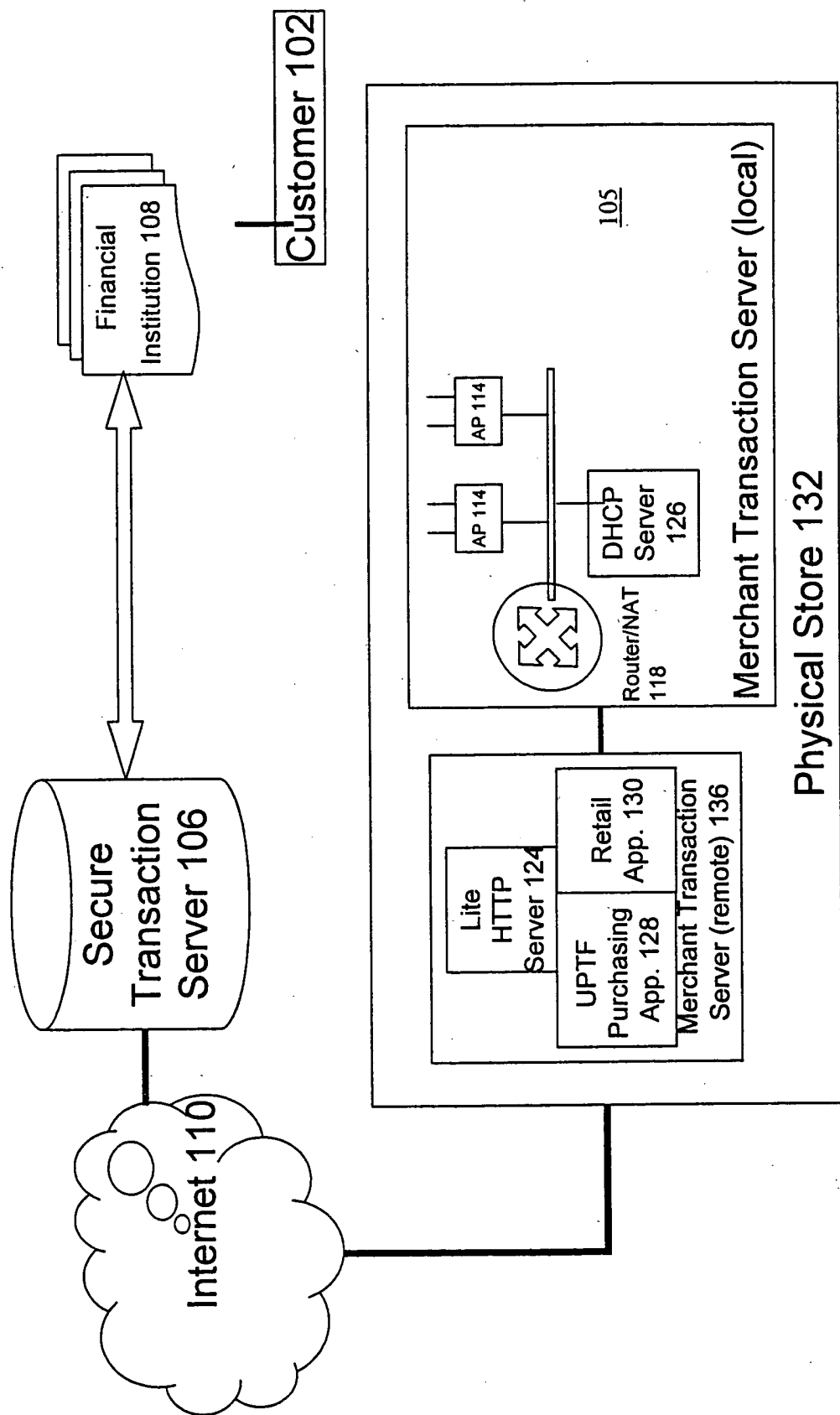


Figure 4

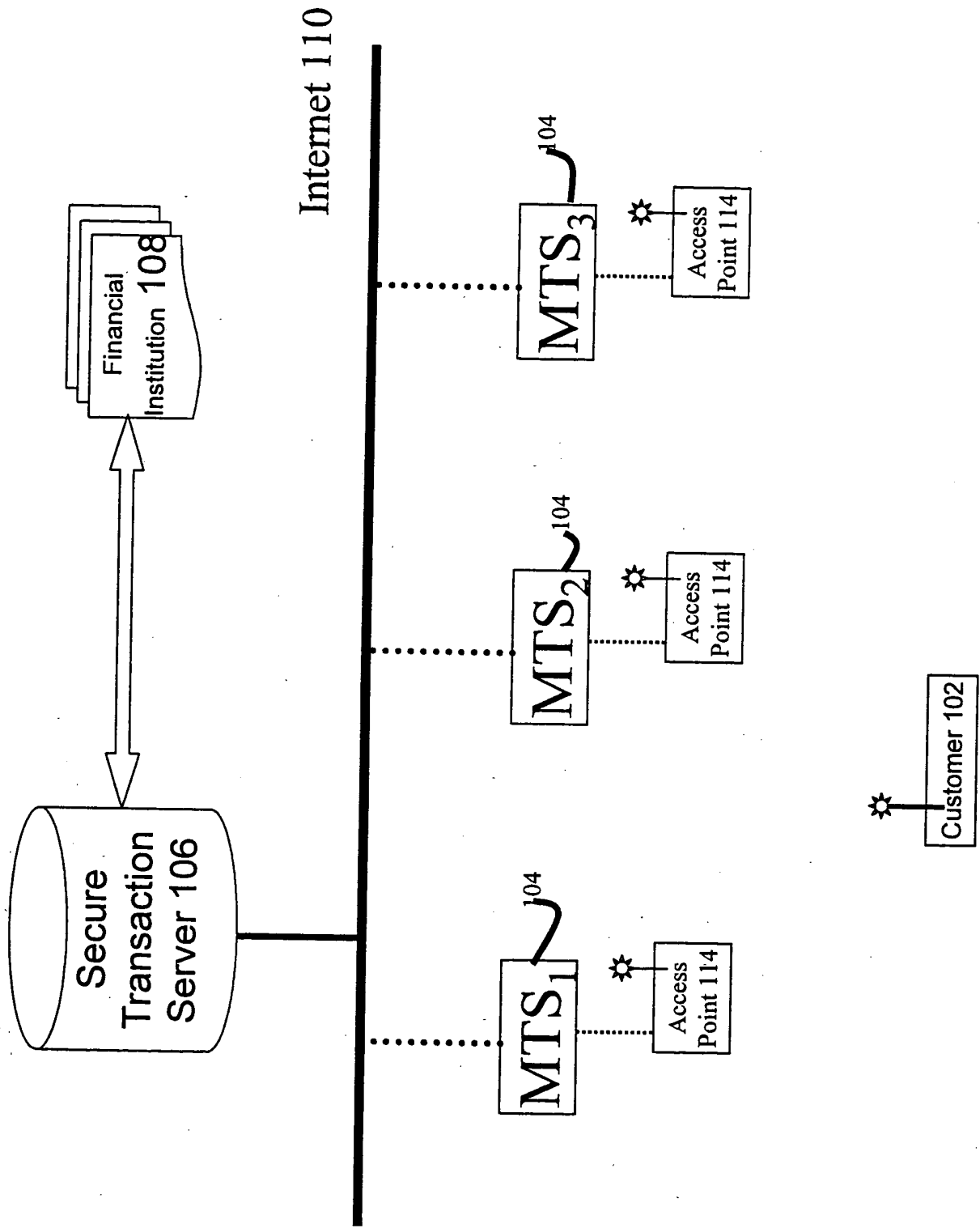


Figure 5

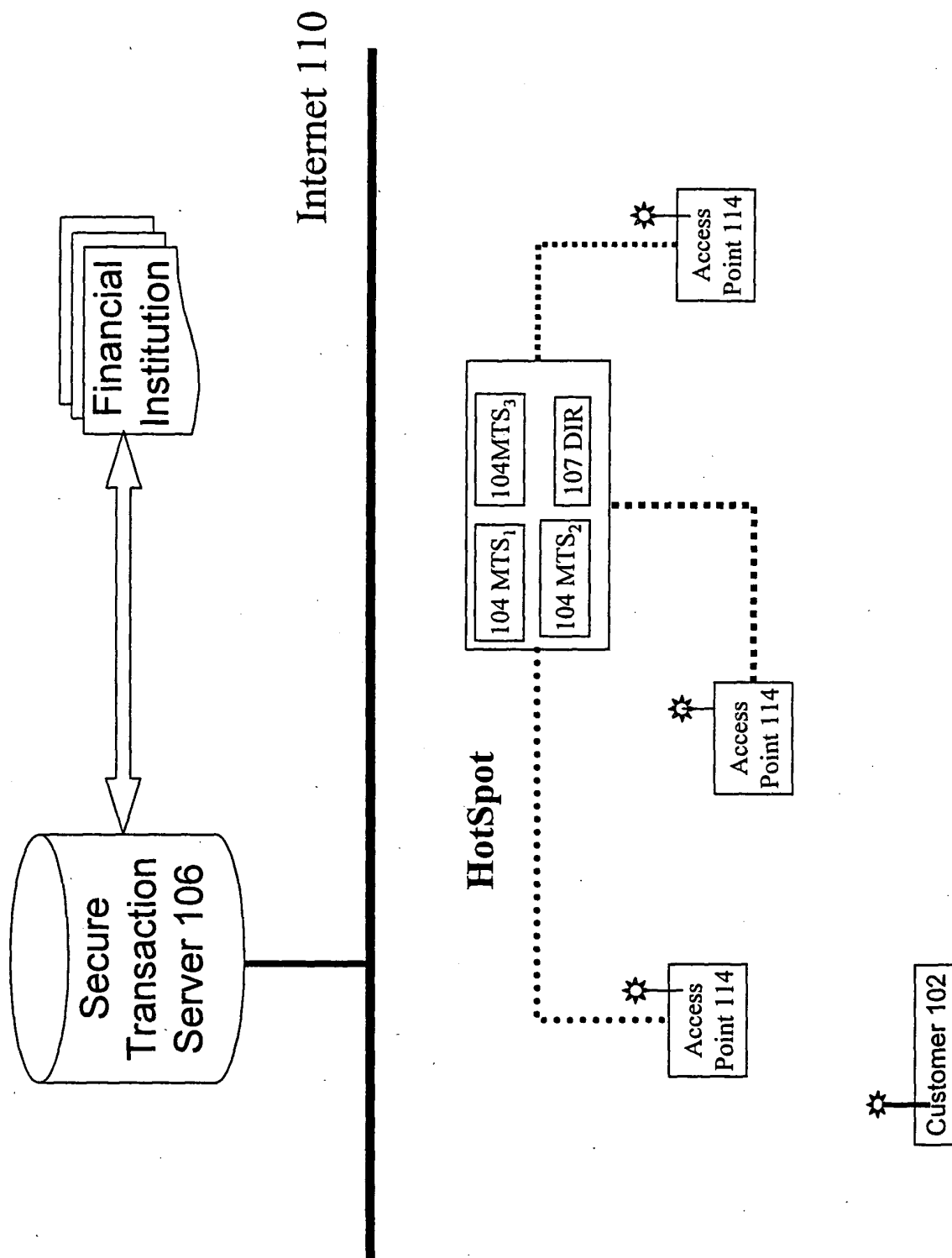


Figure 6

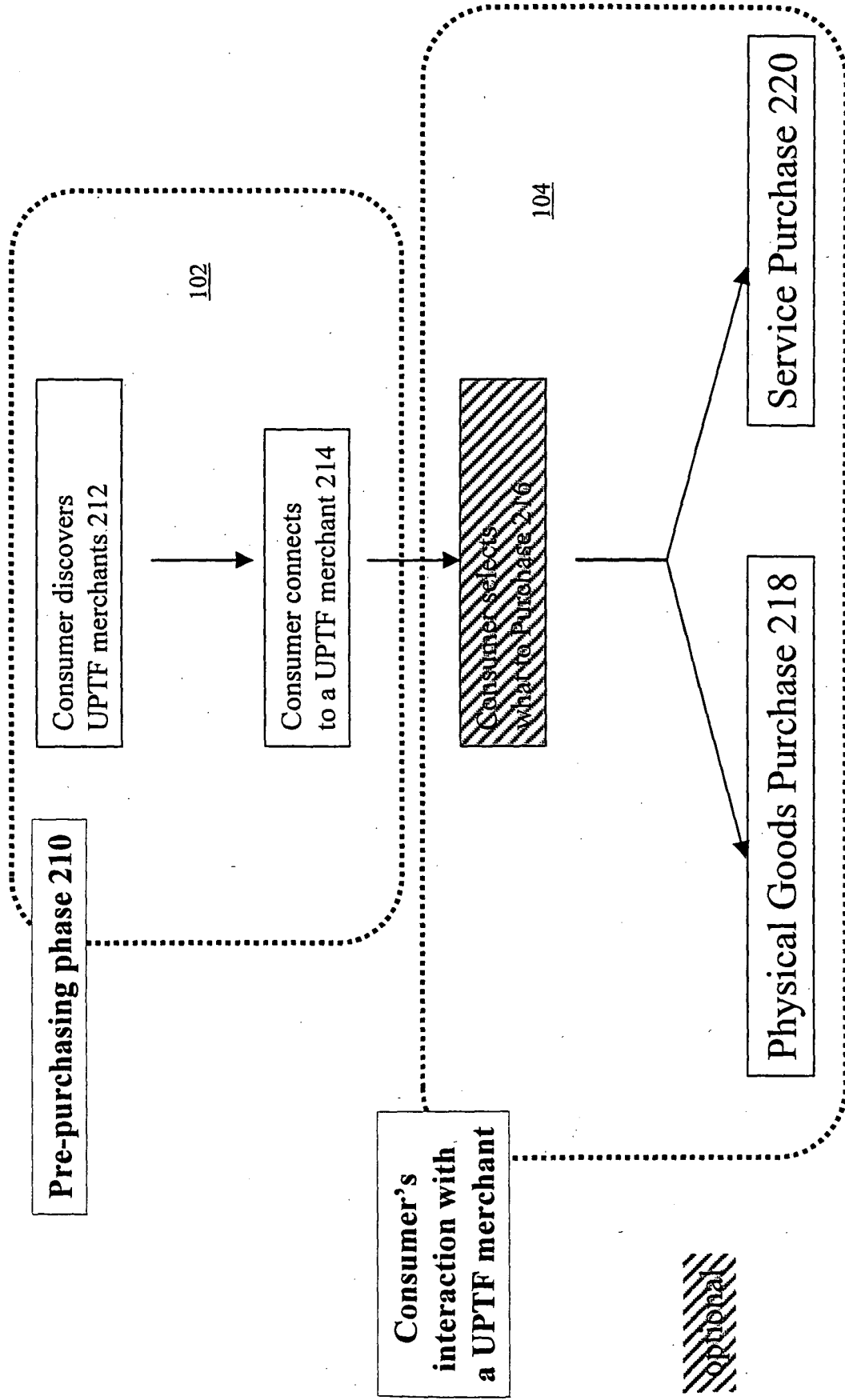
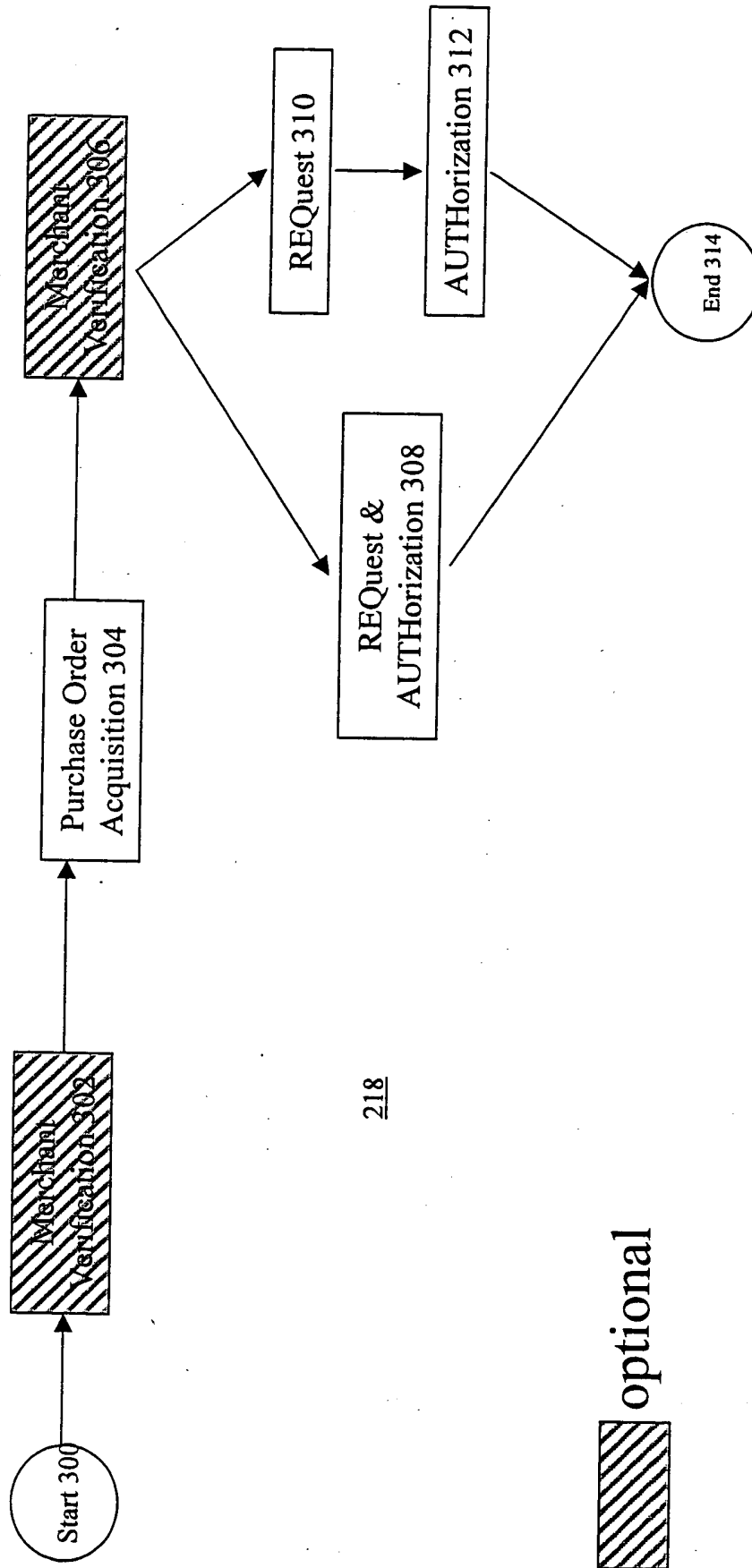


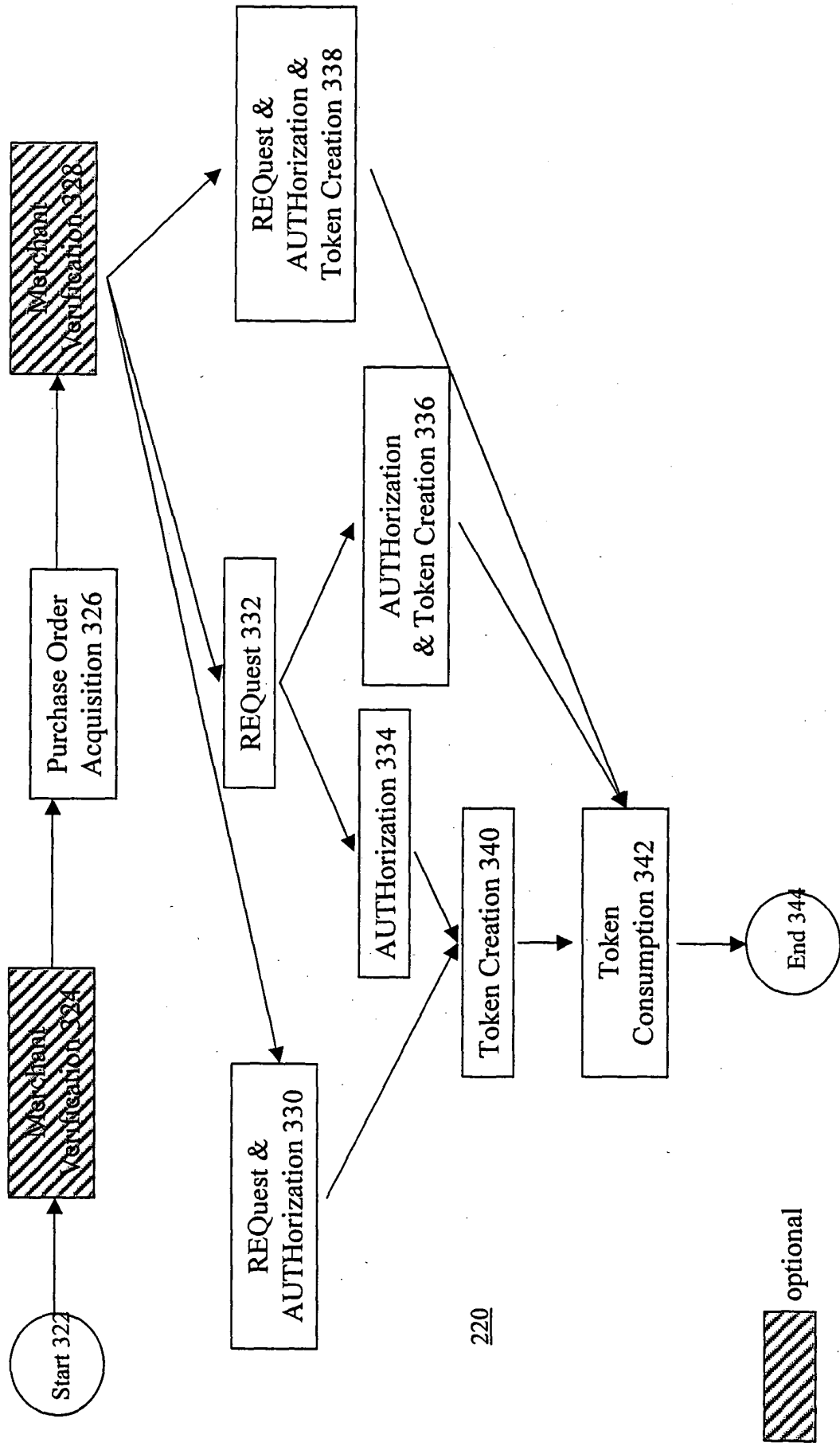
Figure 7



218

optional

Figure 8



220

Figure 9

Consumer 102

Merchant 104

STS 106

350

Consumer requests a
Purchase Order
from merchant

GeneratePurchaseOrder

Merchant generates a
Purchase Order
for a transaction proposal and
returns it to consumer

Purchase Order

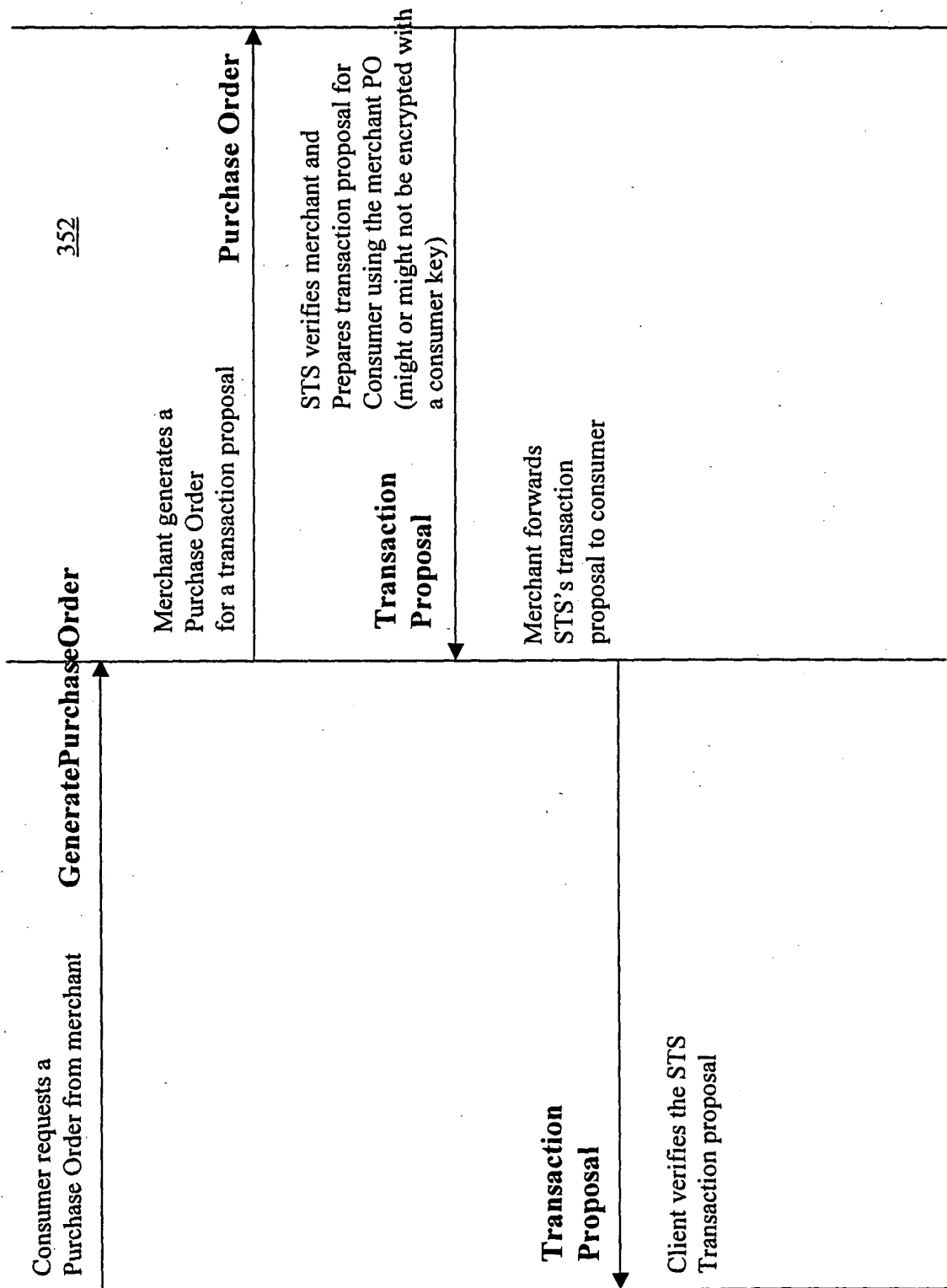
Purchase Order Acquisition - Direct Purchase Order Exchange

Figure 10

Consumer 102

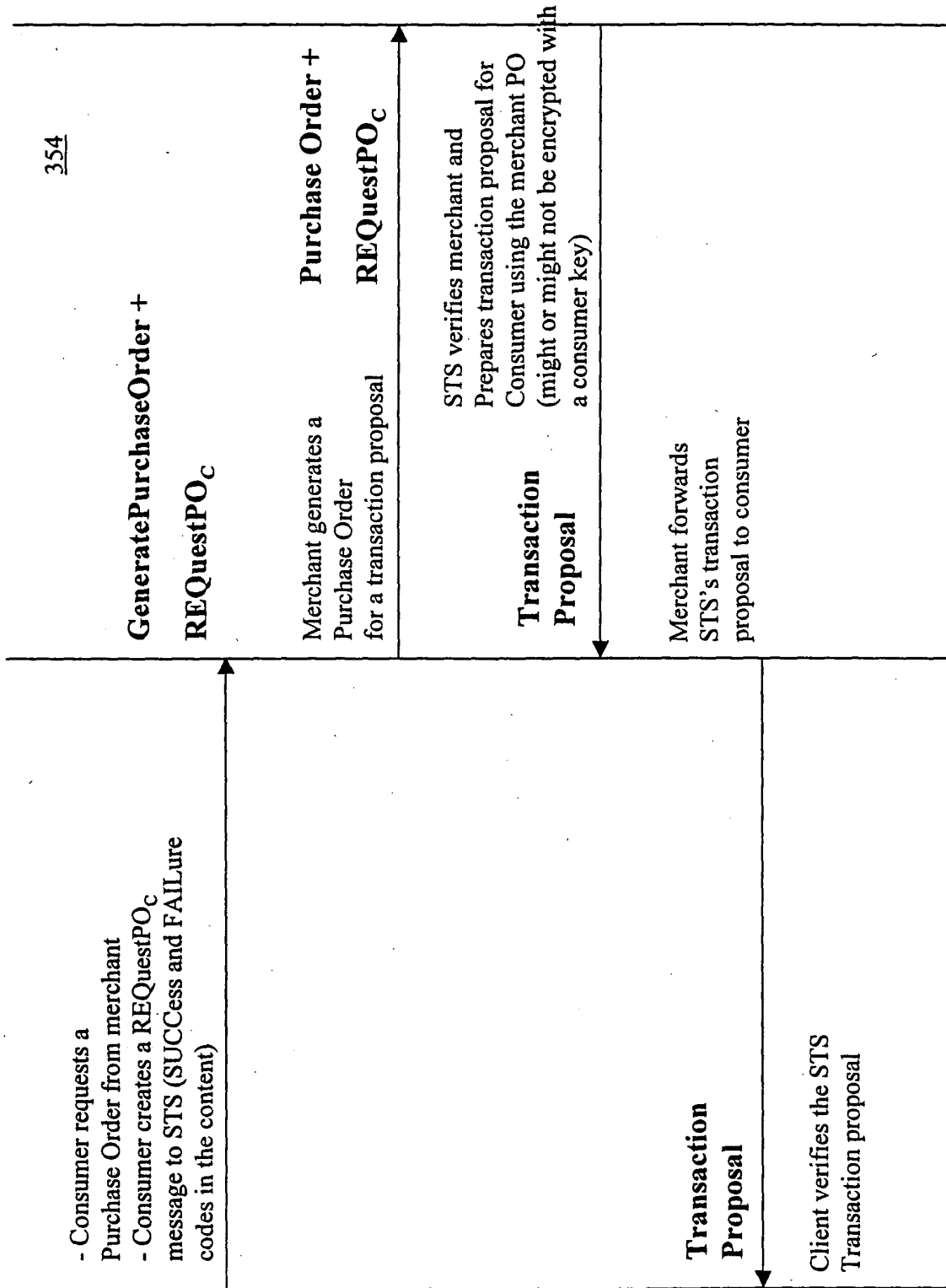
Merchant 104

STS 106



Purchase Order Acquisition – Purchase Order Request

Figure 11



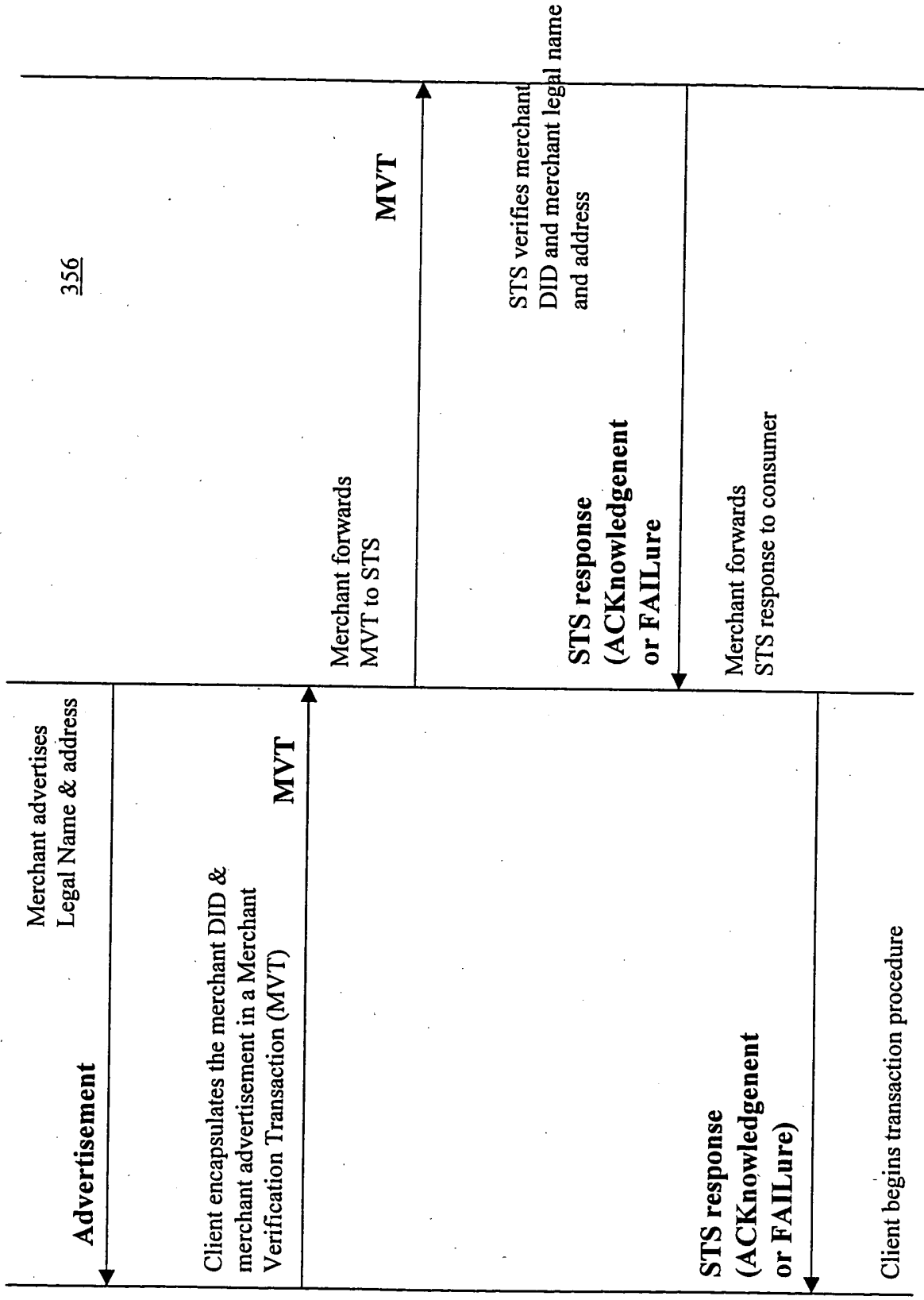
Purchase Order Acquisition – Purchase Order Request from STS

Figure 12

Consumer 102

Merchant 104

STS 106



Merchant Verification

Figure 13

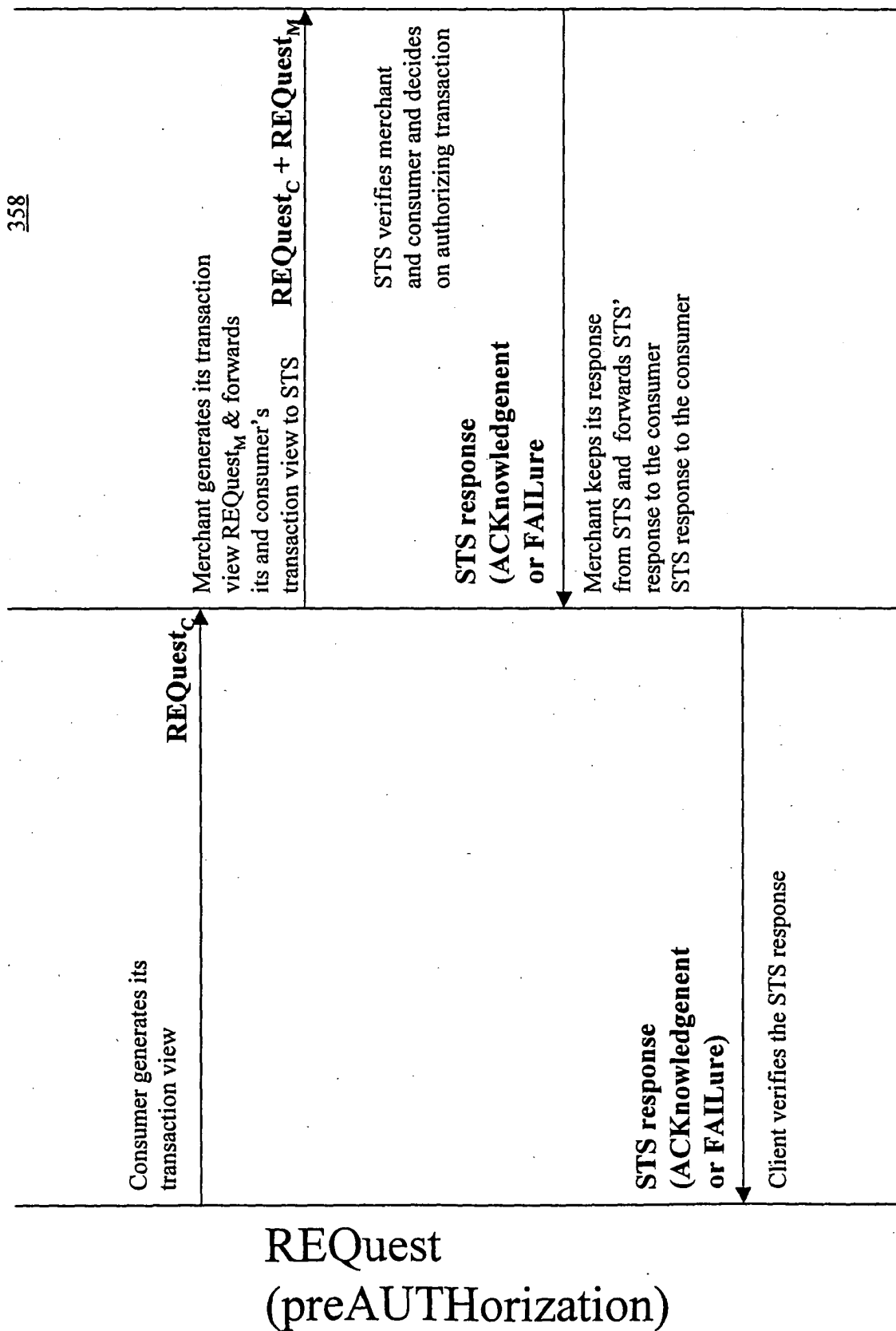


Figure 14

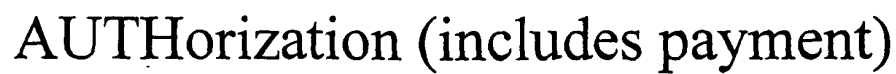


Figure 15

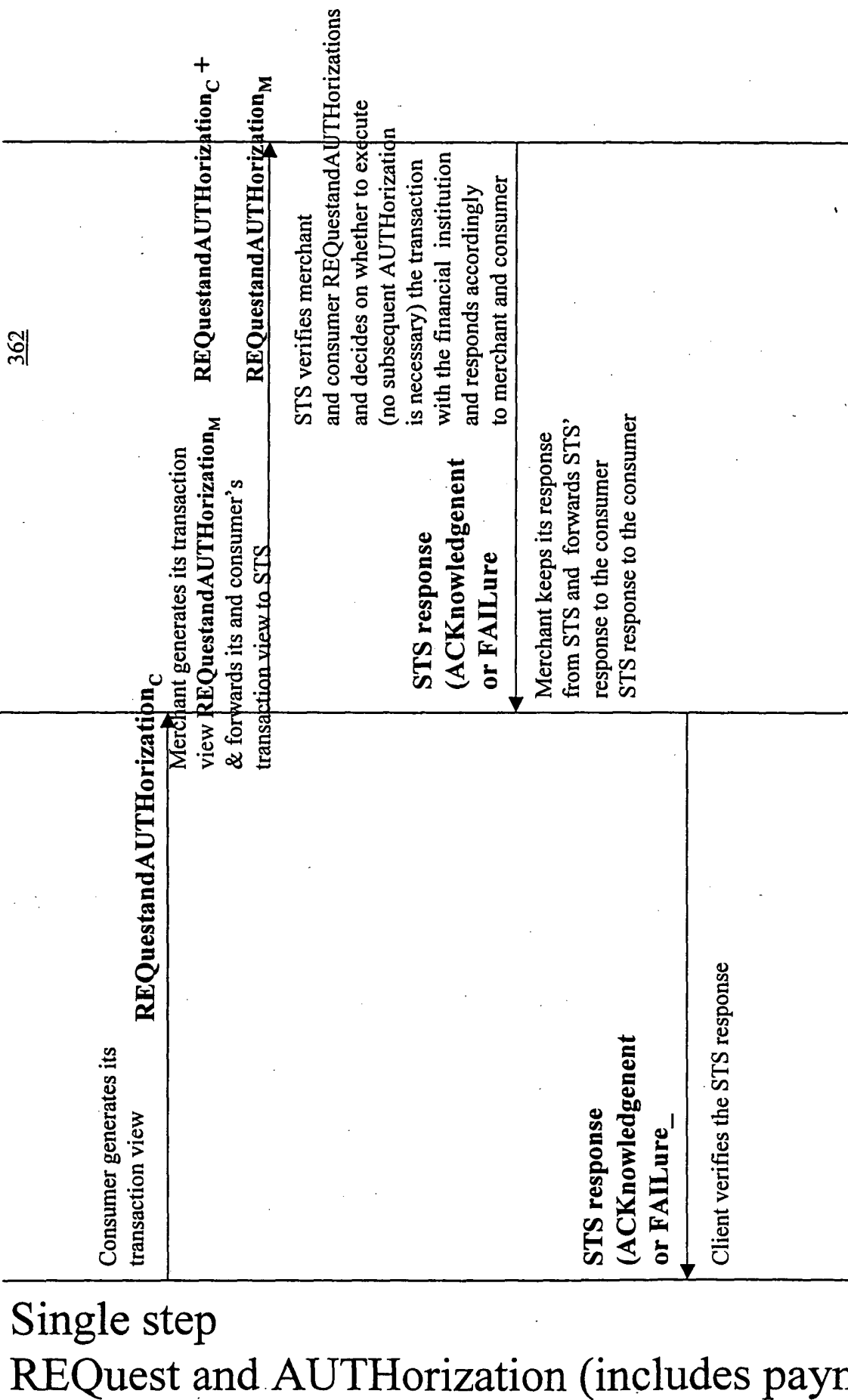


Figure 16

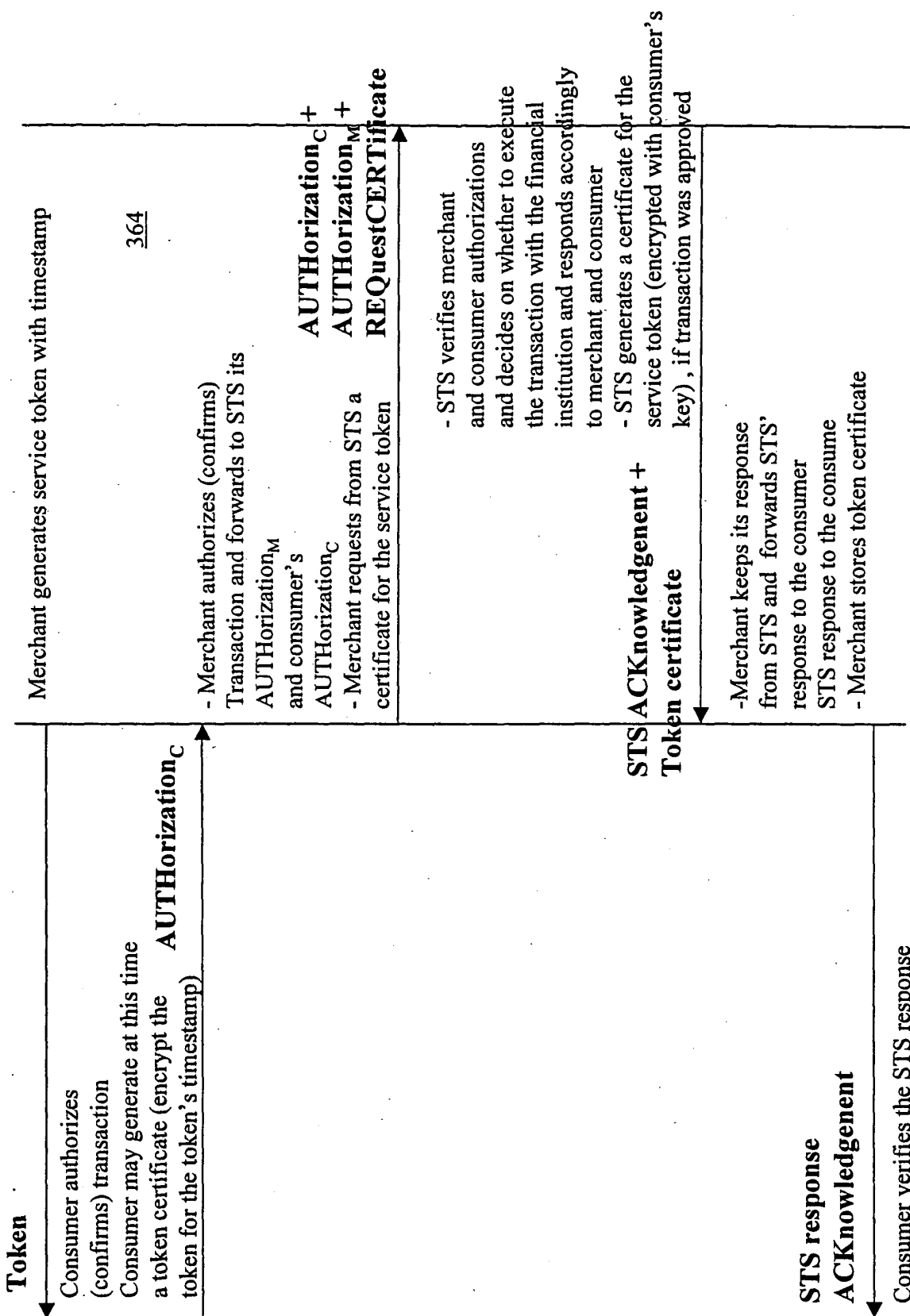
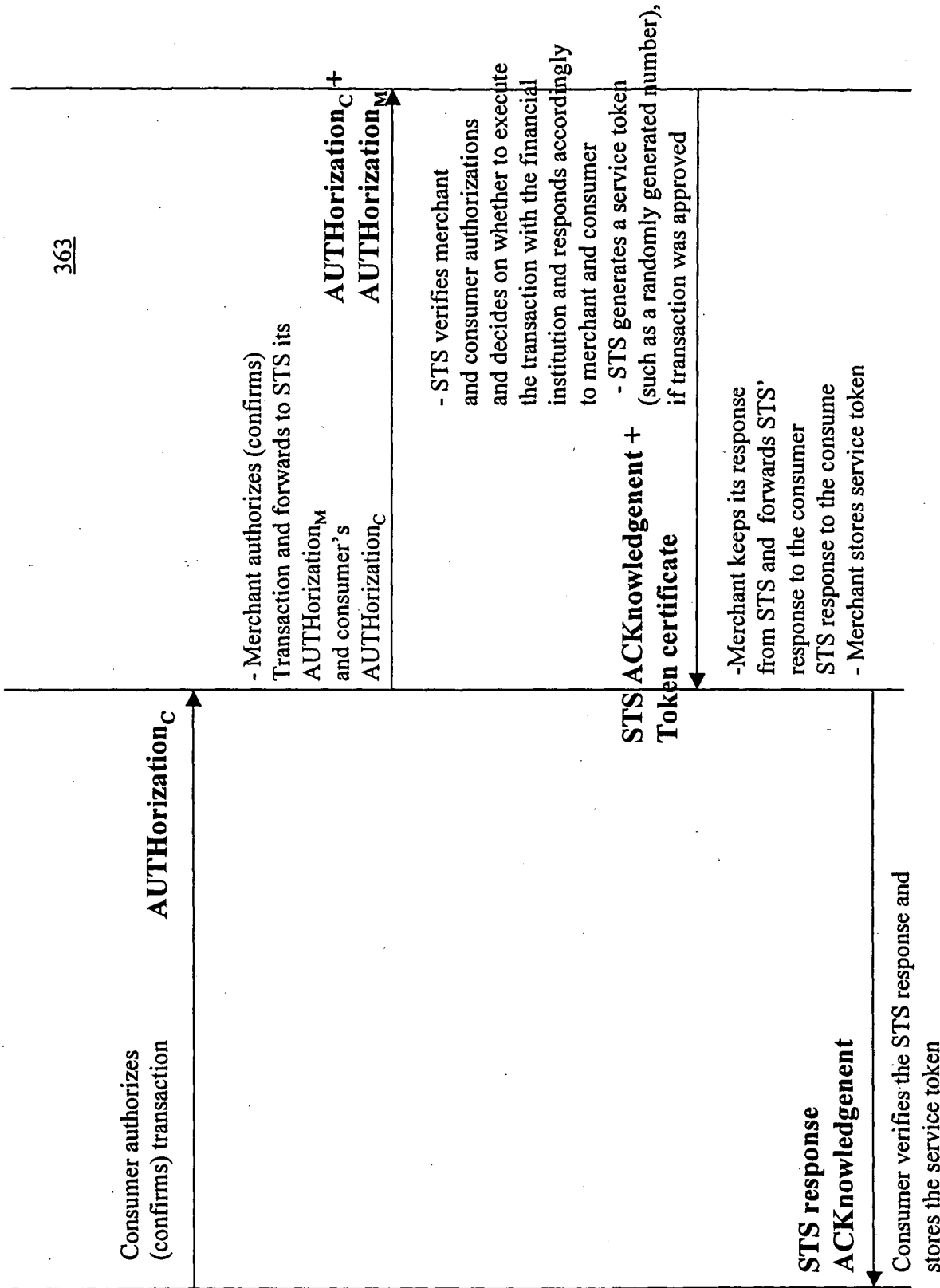
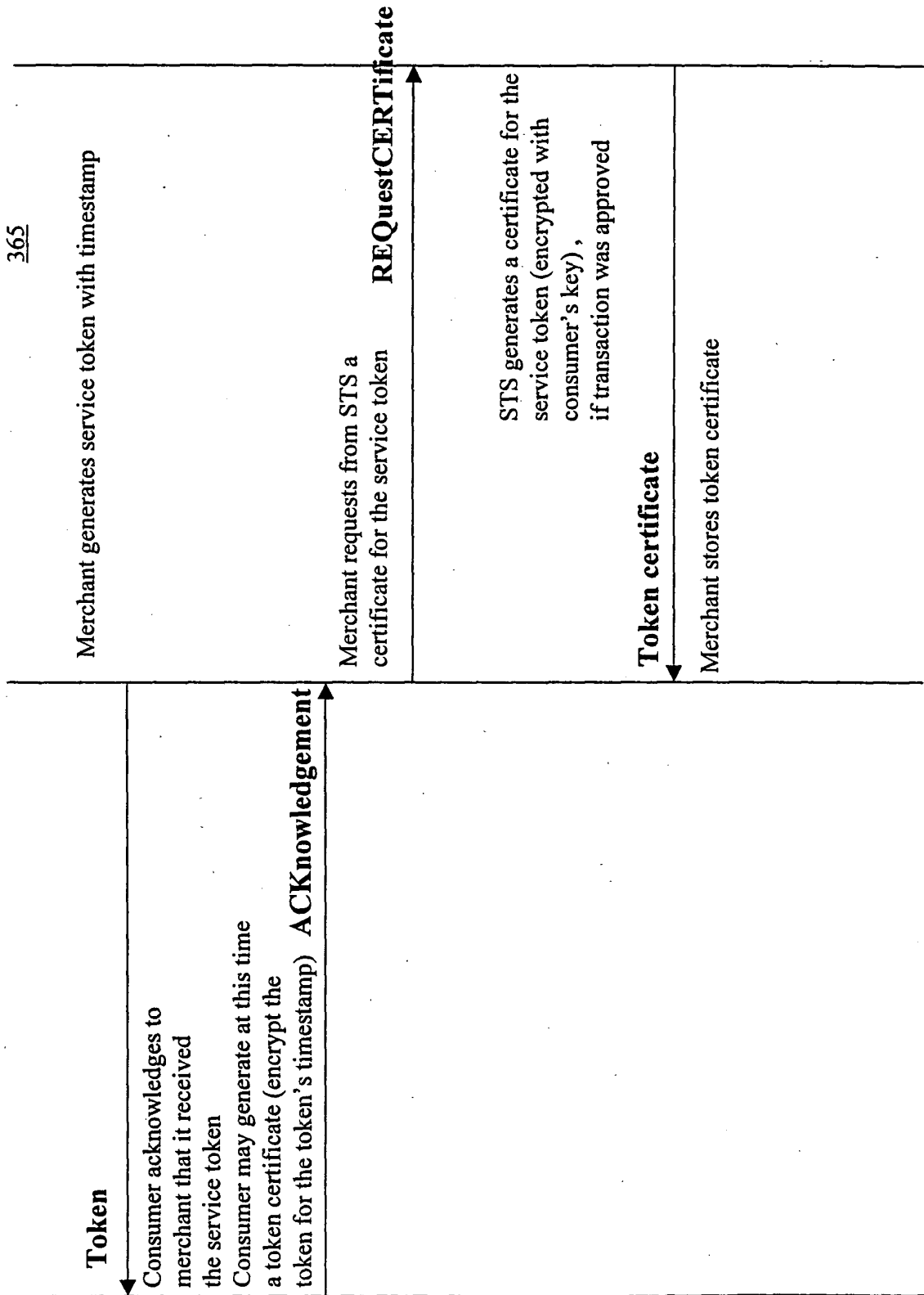


Figure 17



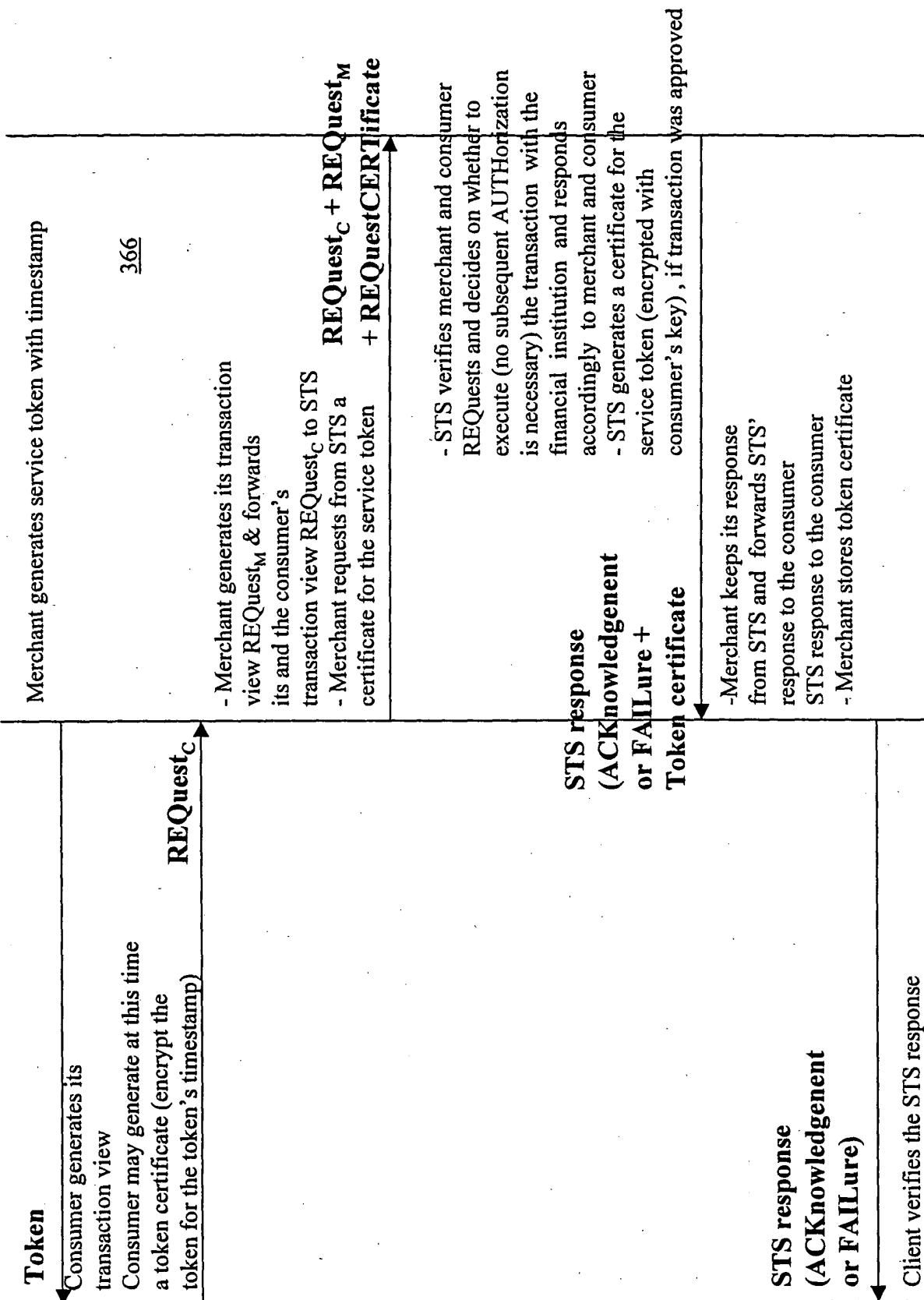
Token Creation and AUTHorization

Figure 18



Token Creation

Figure 19



Single step REQuest, AUTHorization and Token Creation

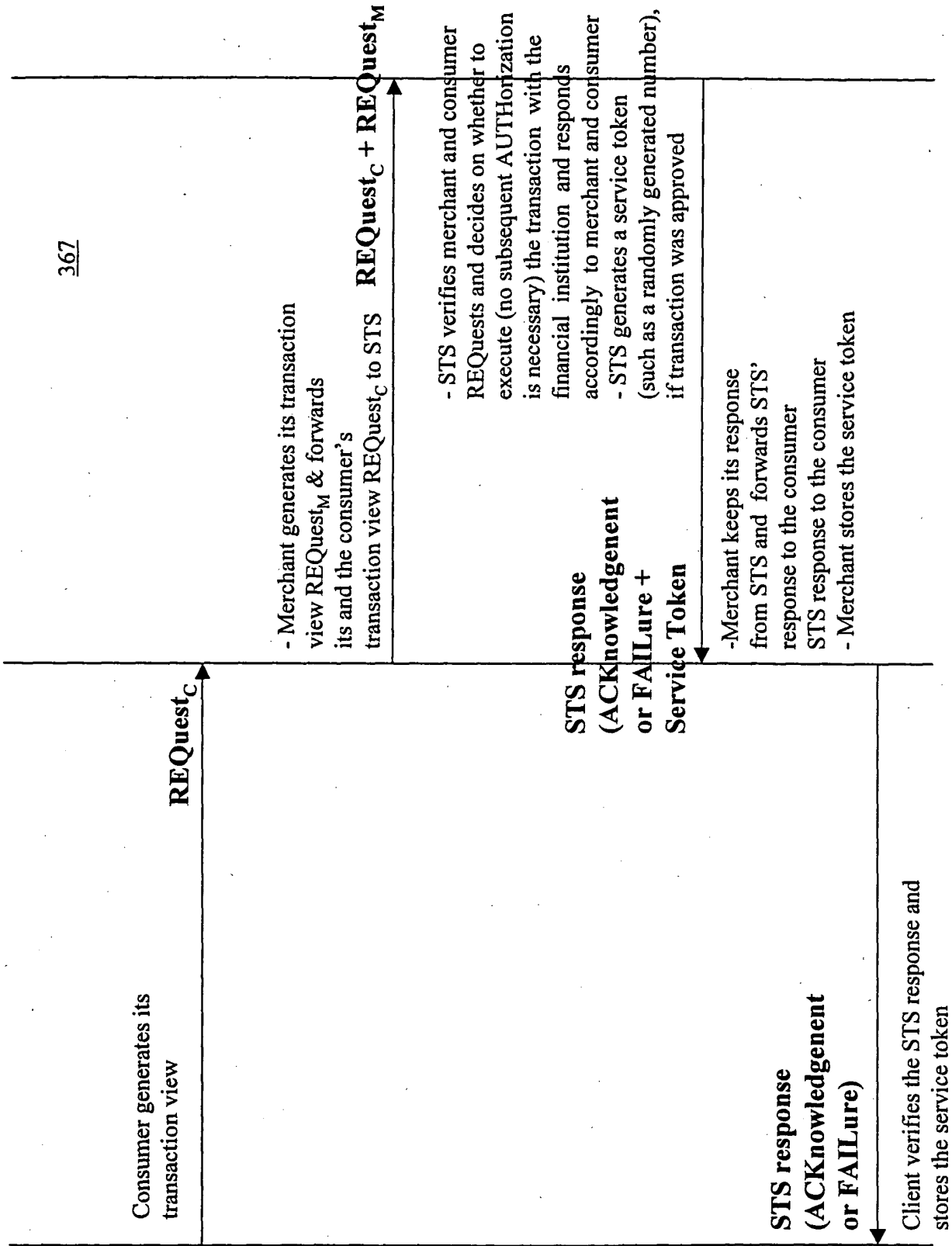
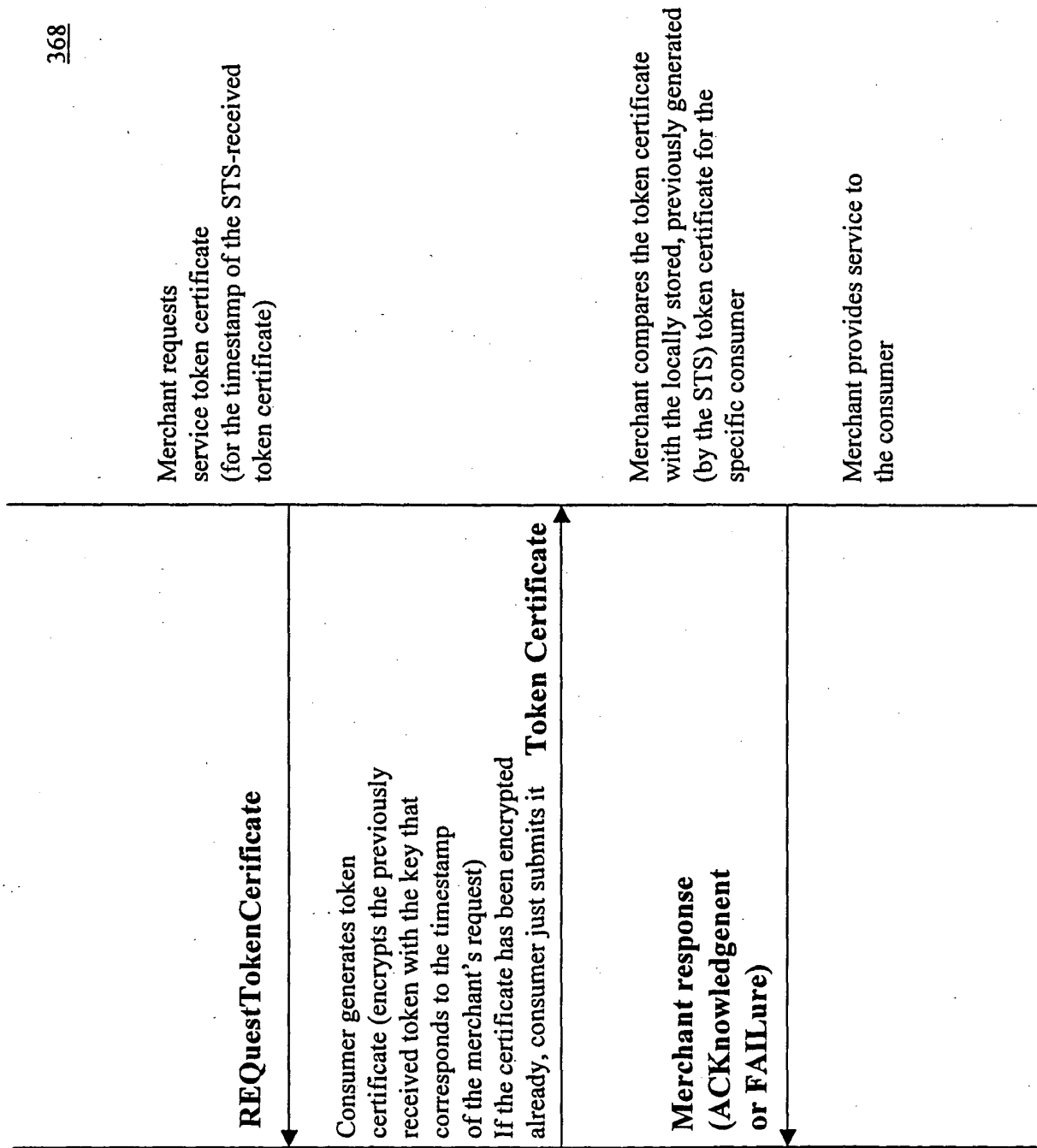


Figure 21

Single step REQuest, AUTHorization and Token Creation



Service Token Verification and Consumption

Consumer 102

Merchant 104

STS 106

370

Token Creation

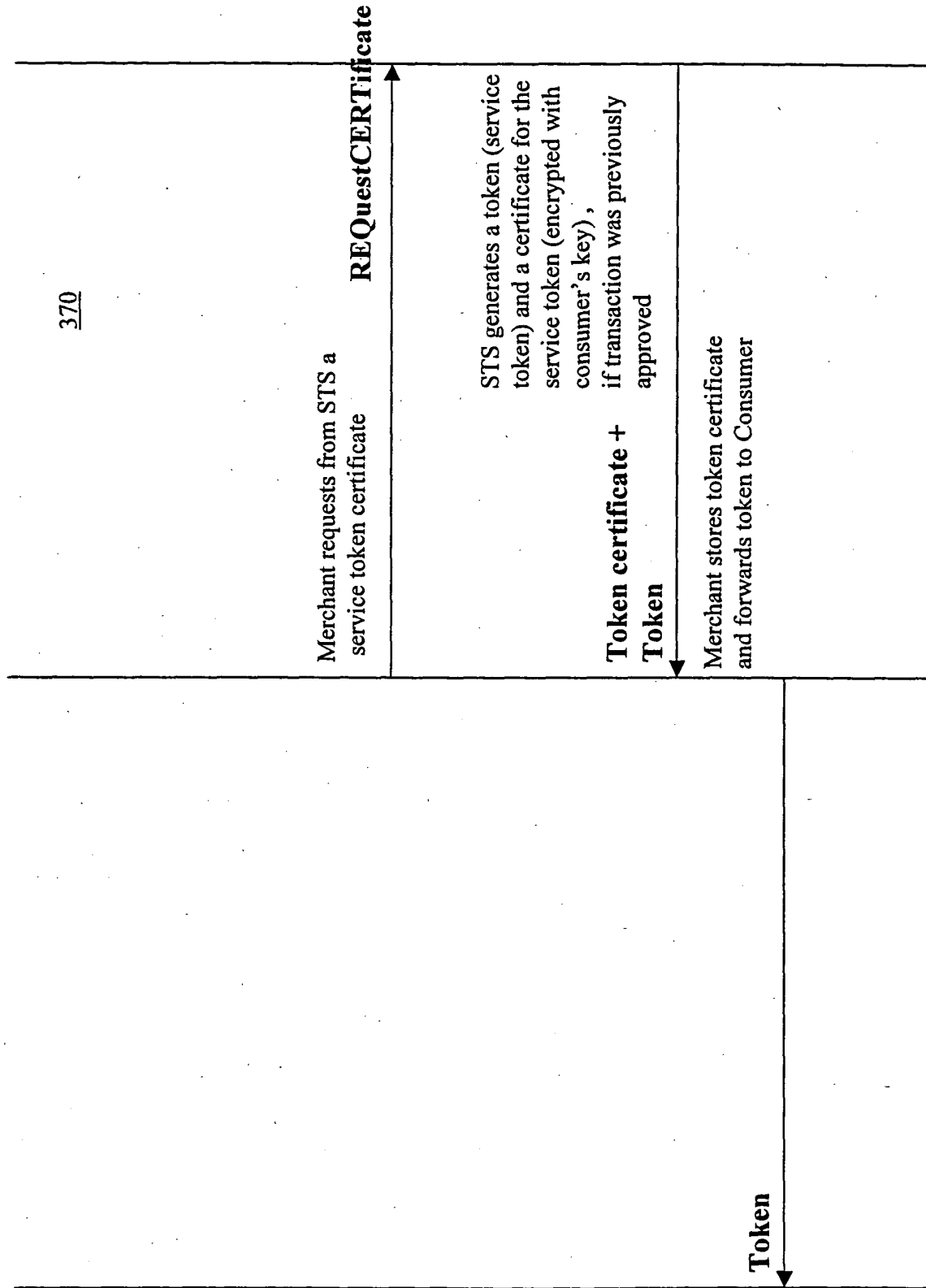


Figure 23

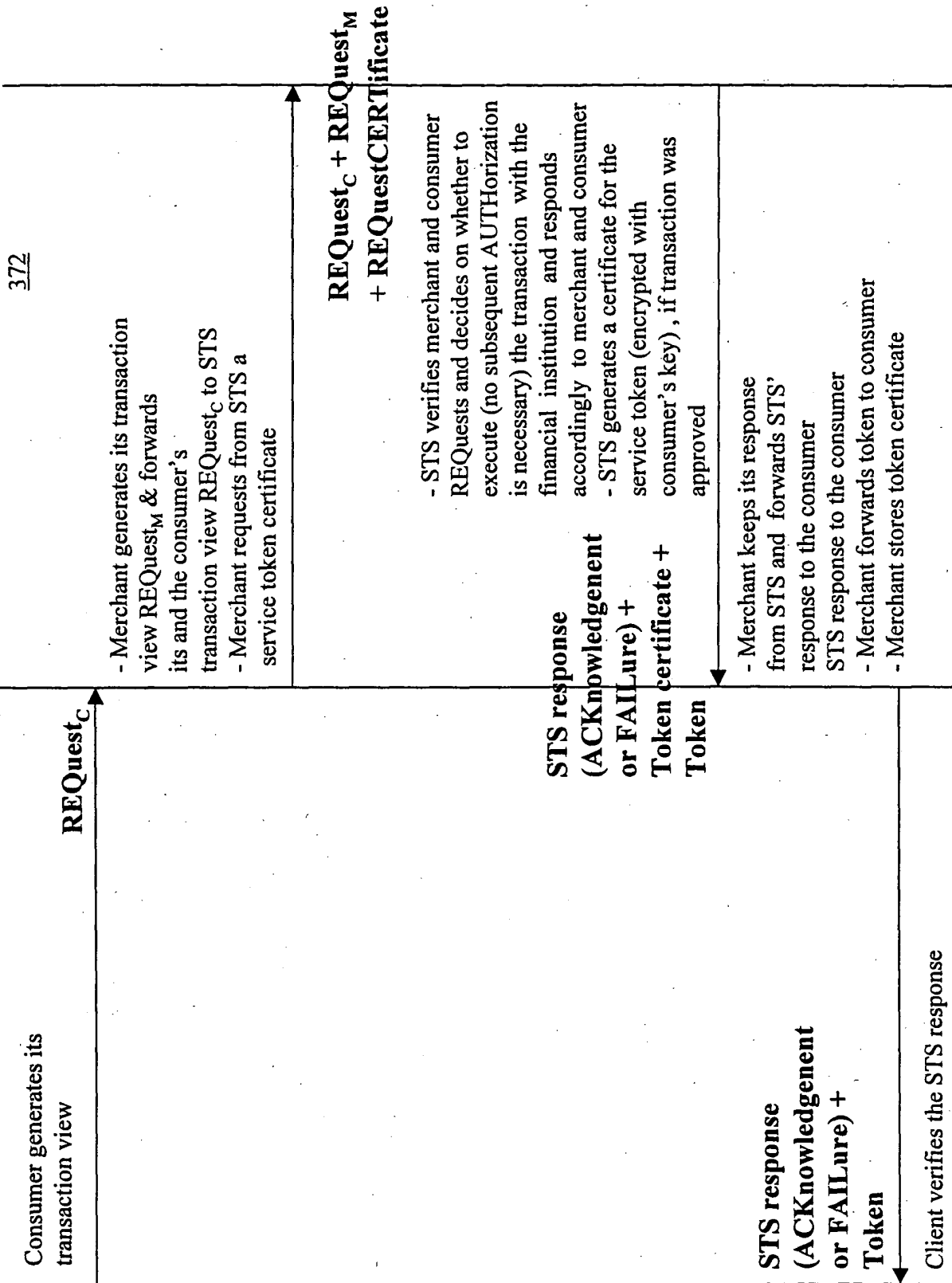
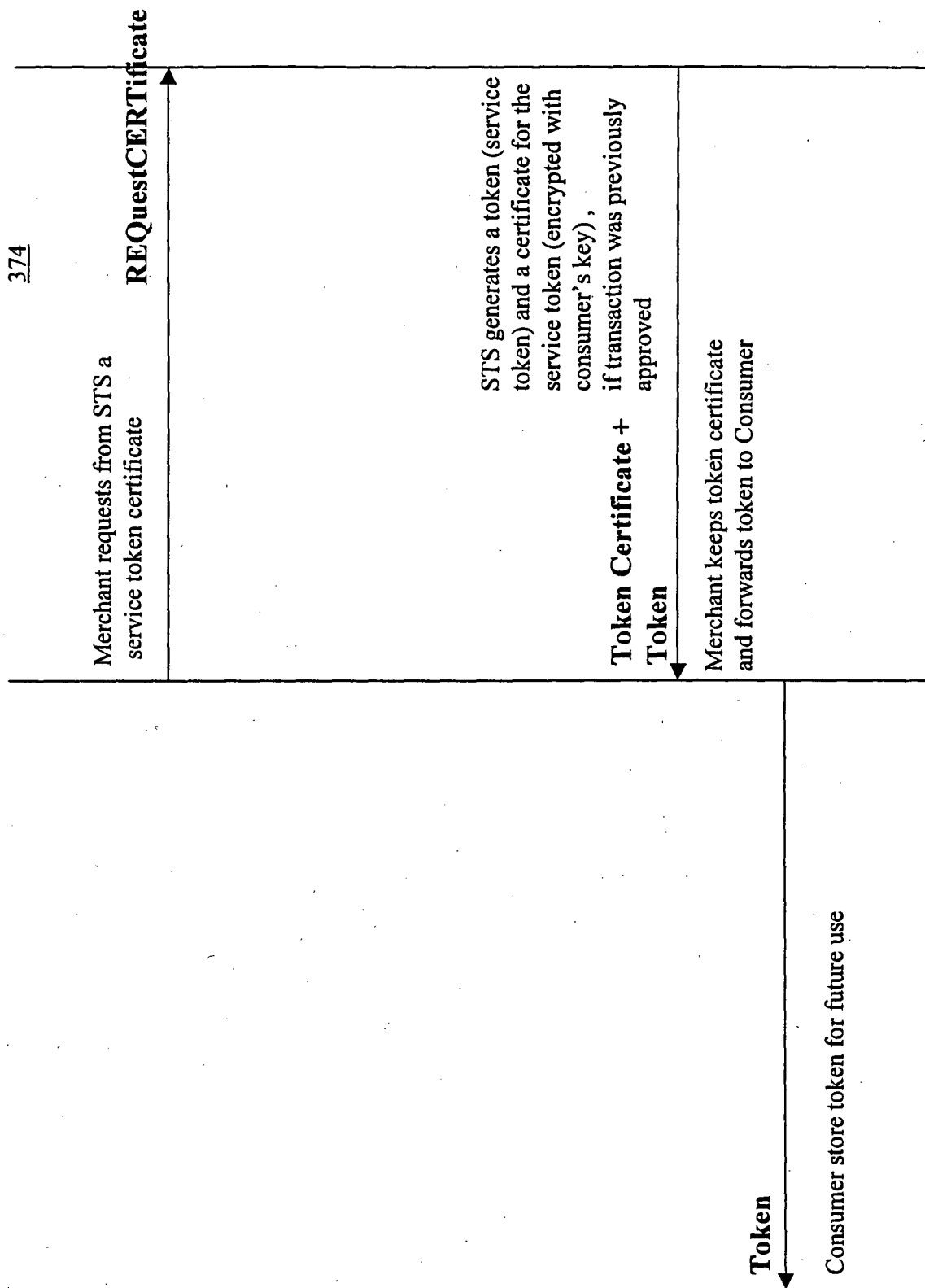


Figure 24

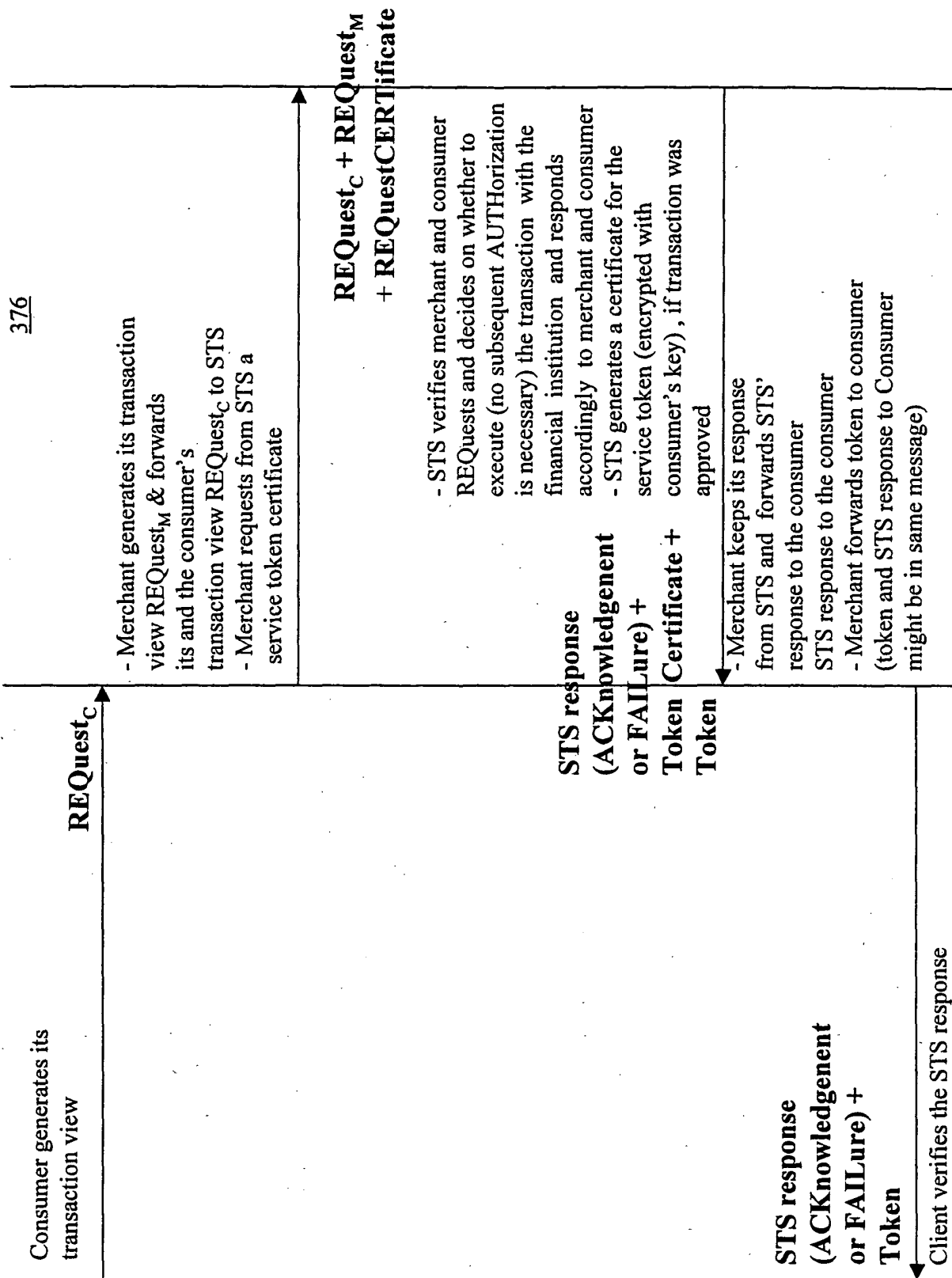
Single step $REQuest$, $AUTHORIZATION$ and Token Creation
(for token certificate verification by STS)



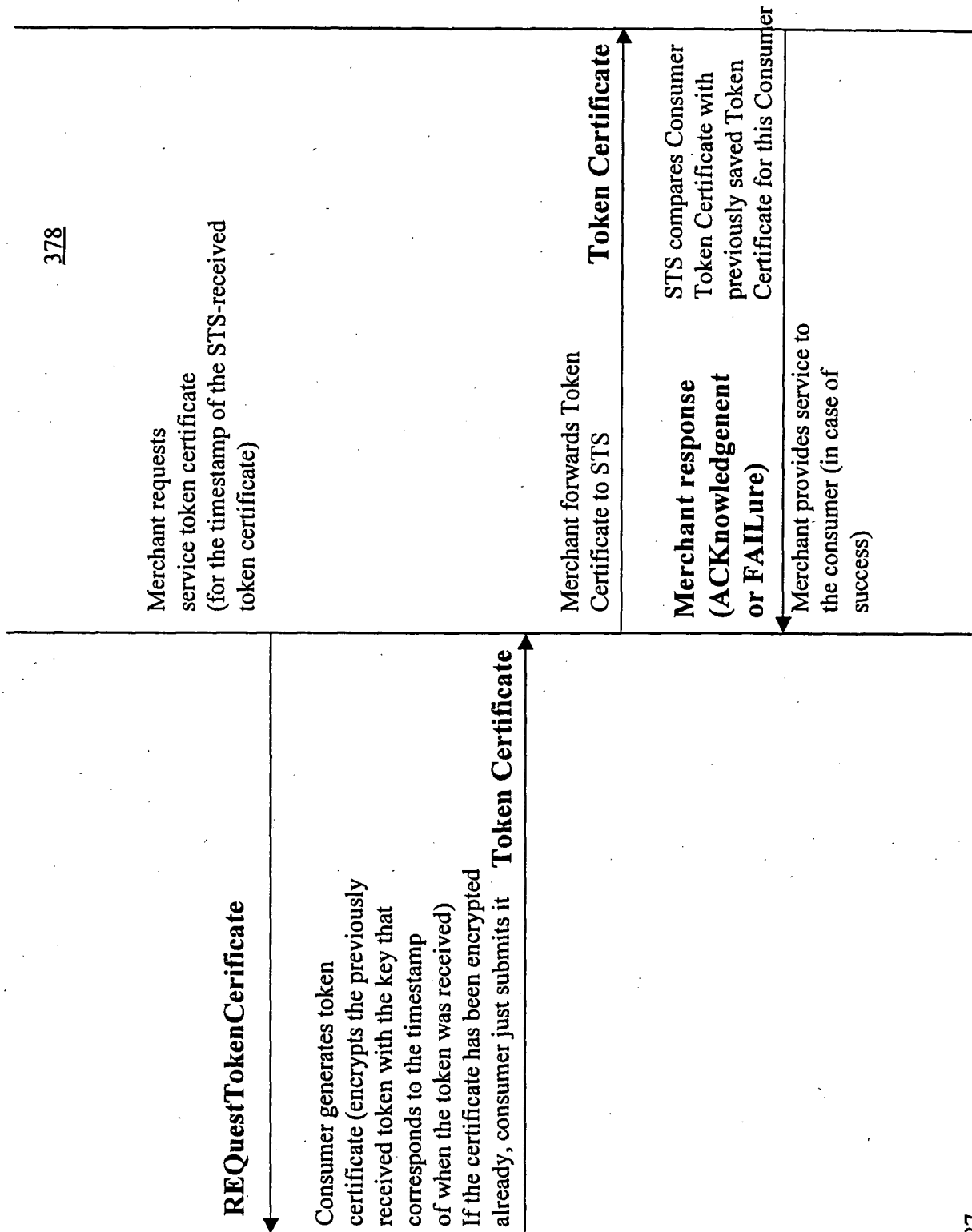
Token Creation

(for token certificate verification by STS)

Figure 25



Single step $REQuest$, $AUTHORIZATION$ and Token Creation
(for token certificate verification by STS)

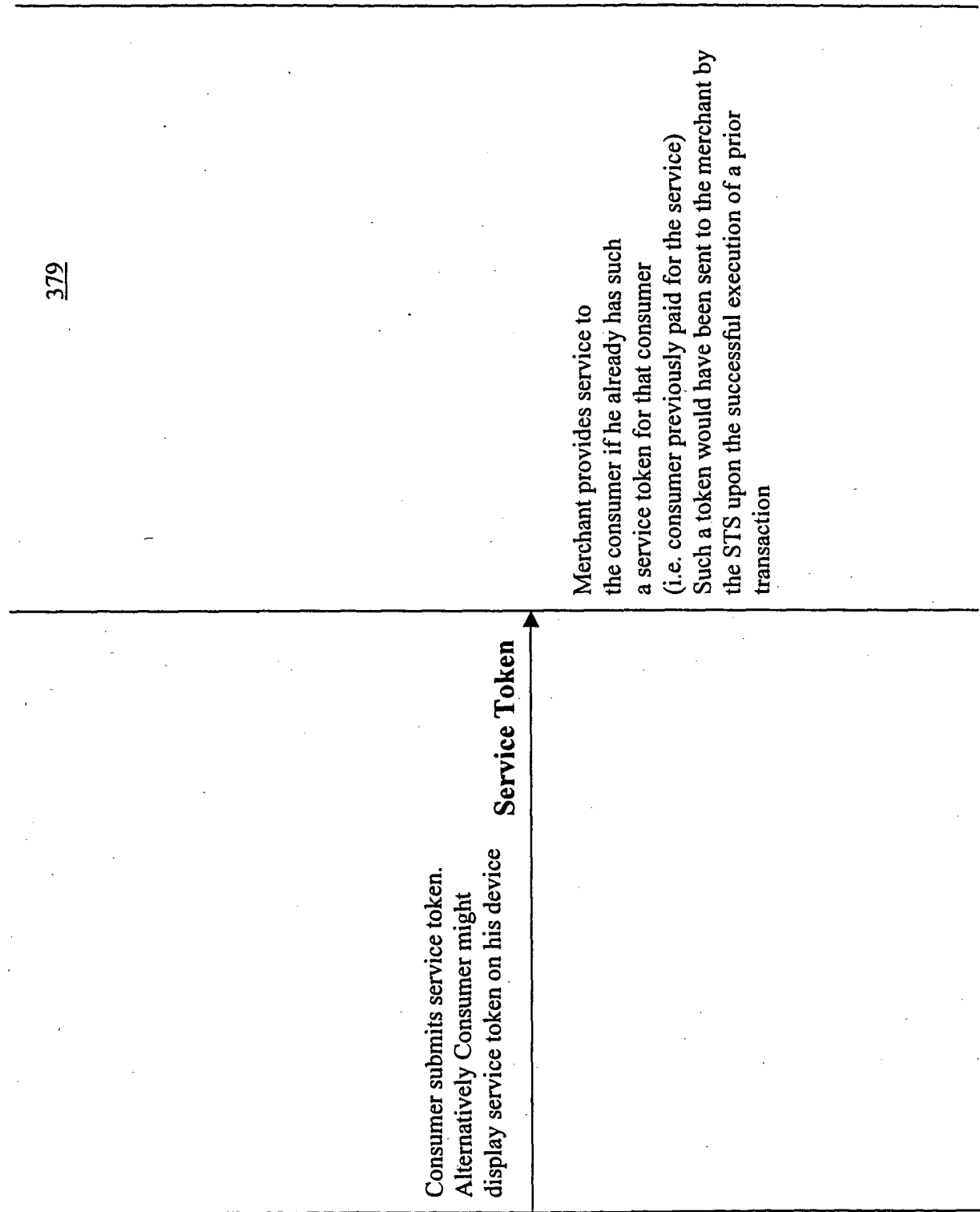


Service Token Consumption (Verification by STS)

Consumer 102

Merchant 104

STS 106



Service Token Consumption (Verification by Merchant only)

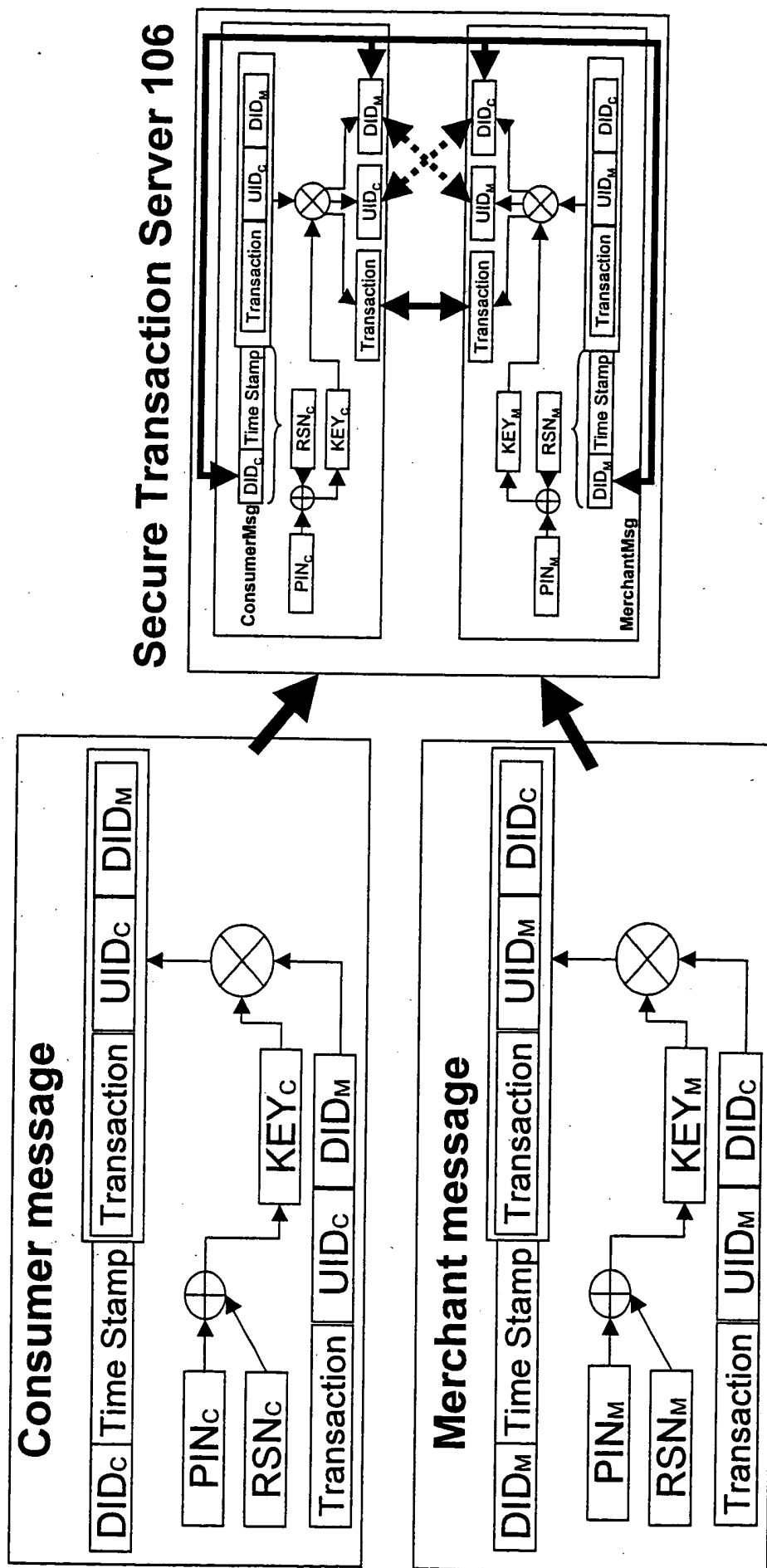


Figure 29

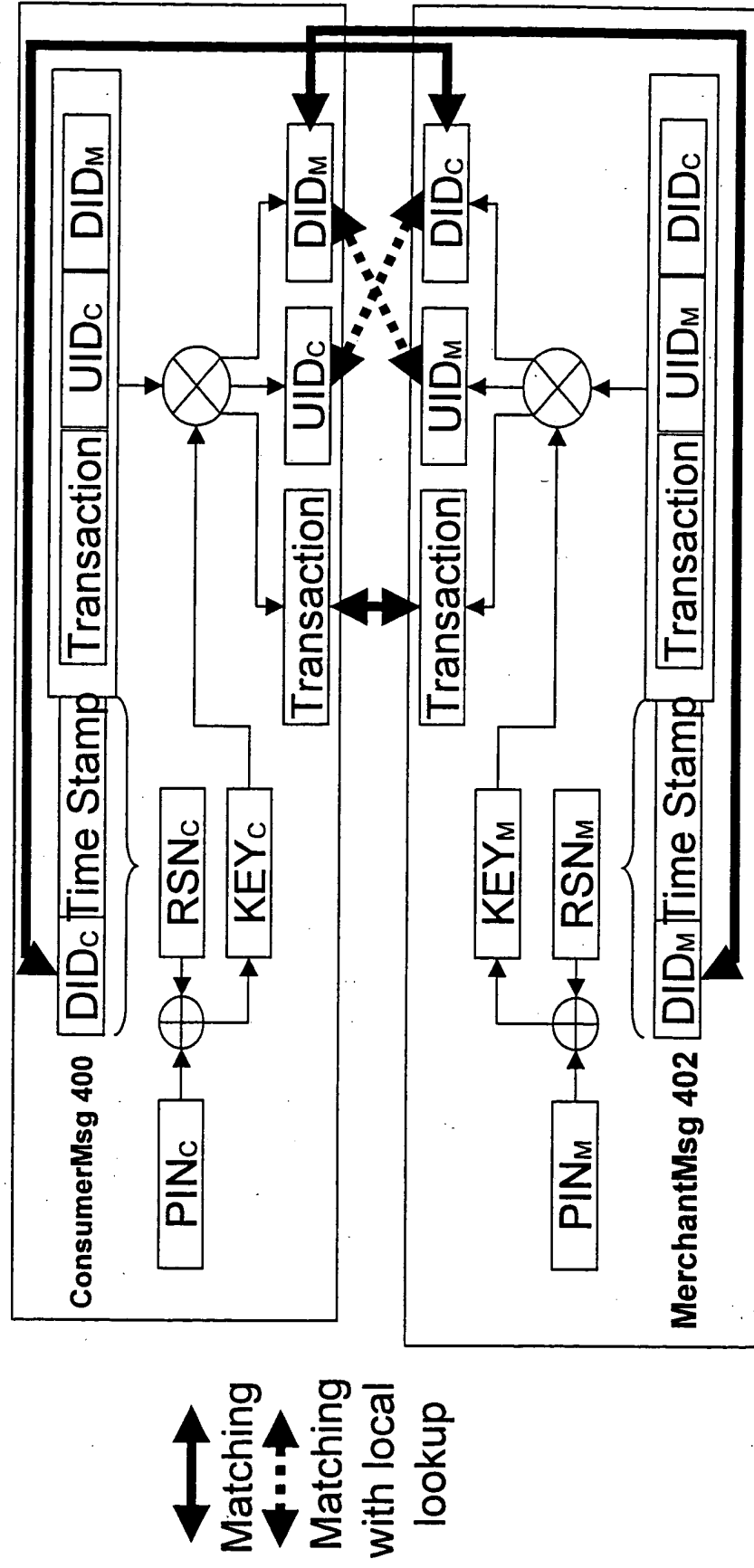


Figure 30

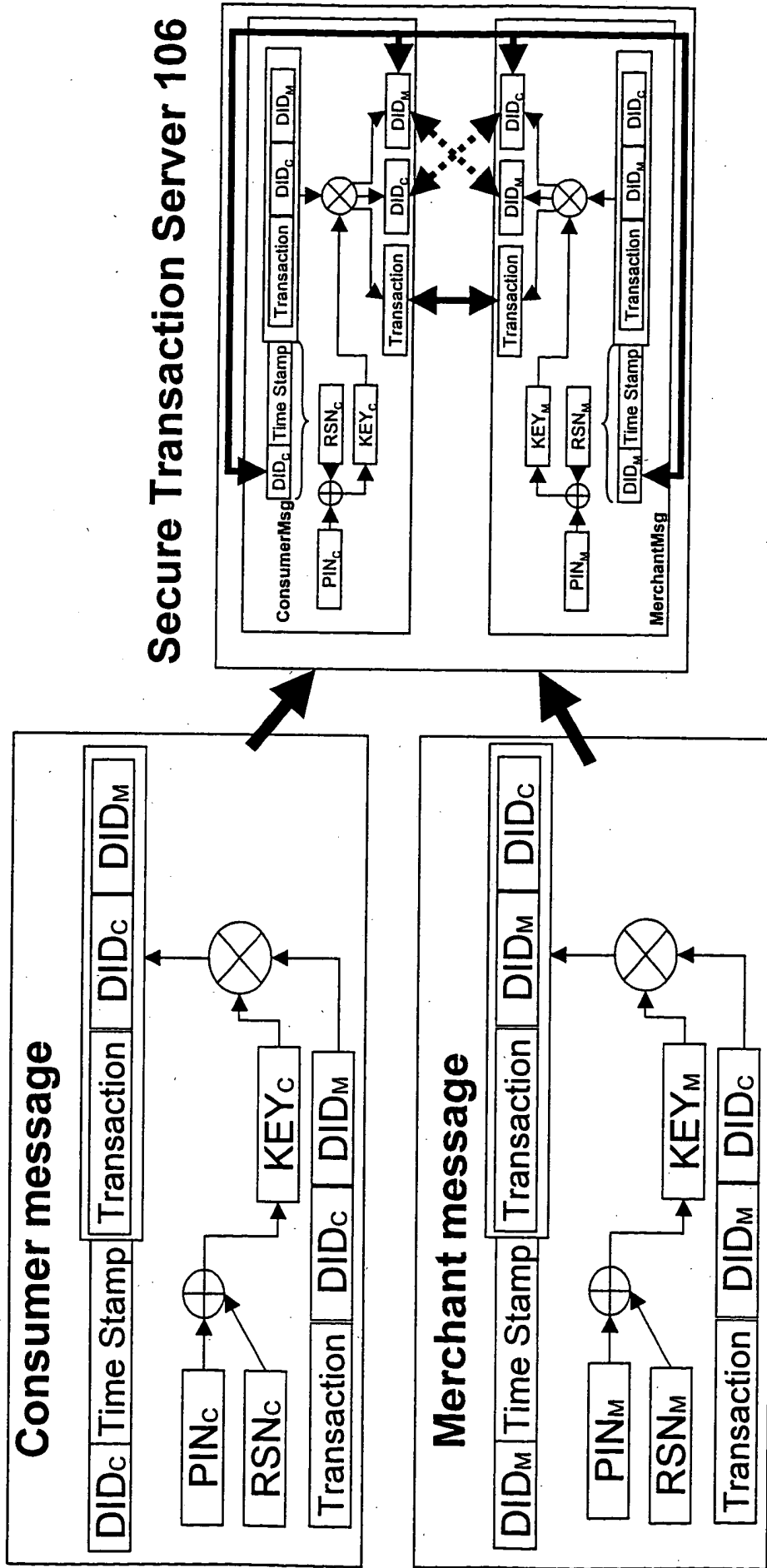


Figure 31

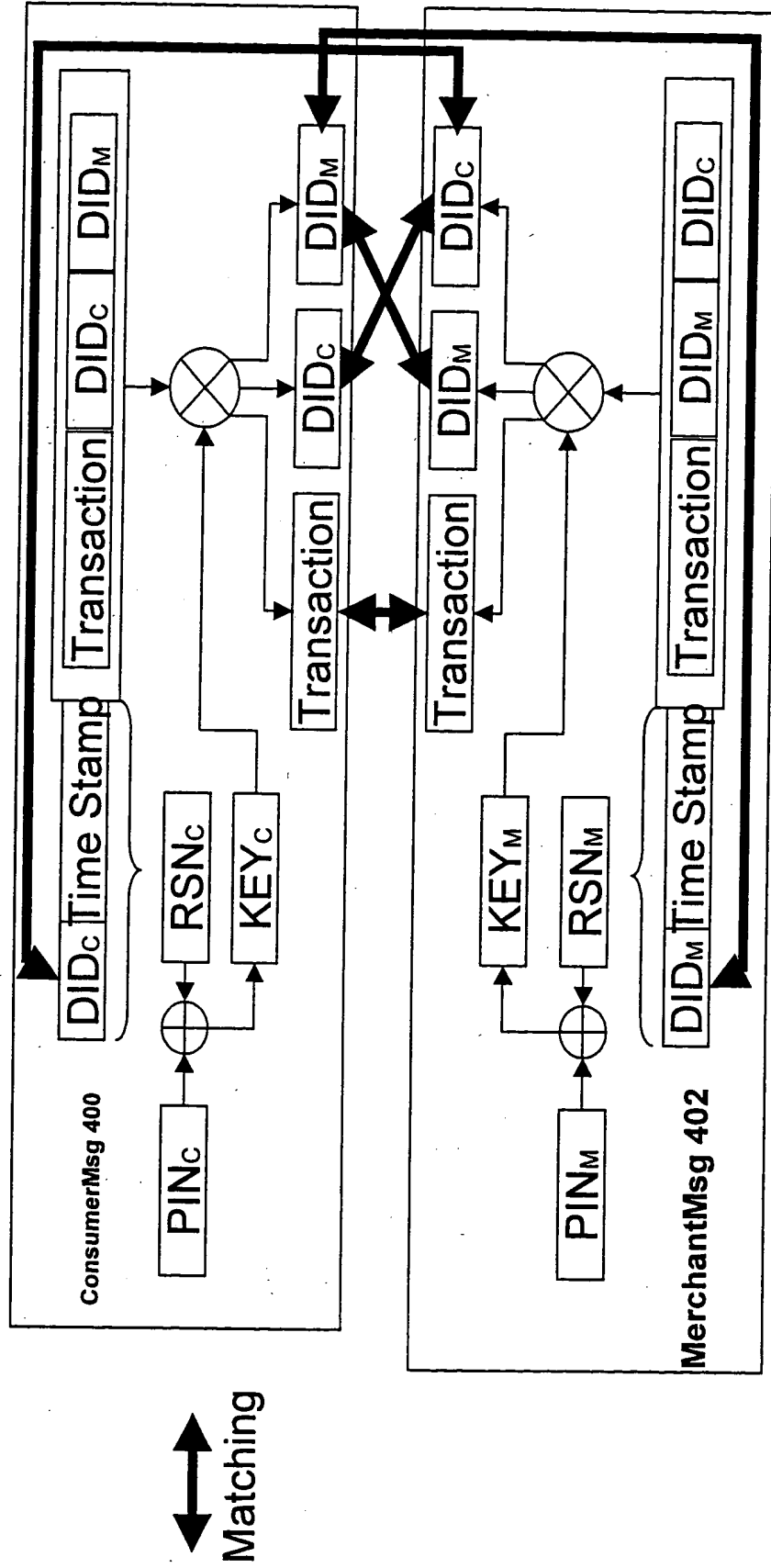
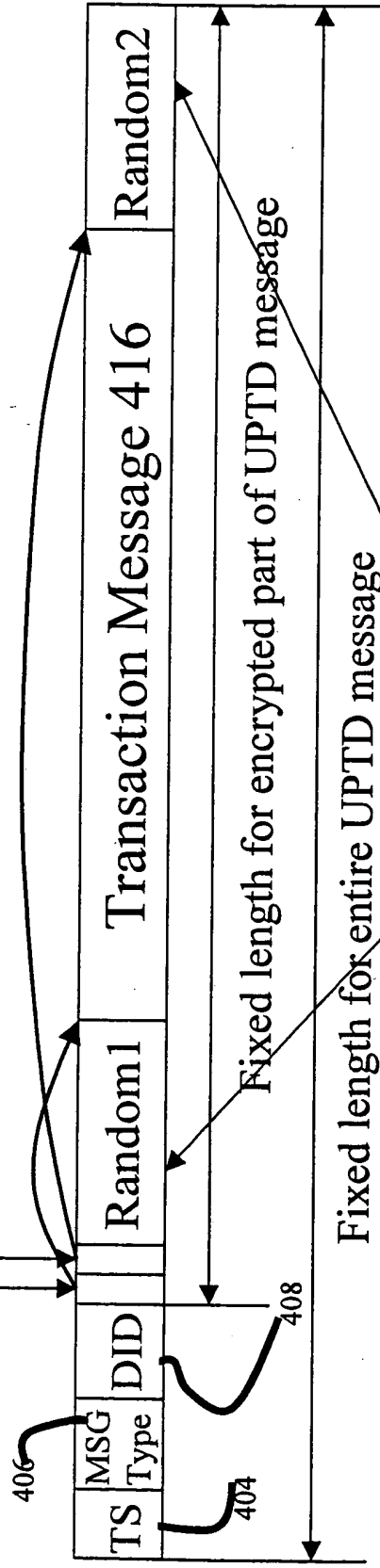


Figure 32

Pointer 412 to end of Transaction Message or Transaction Message Length or Length of Random2

Pointer 410 to beginning of Transaction Message or Length of Random1



400

Length of each "Random" section is random and decided at the time of message composition.

414: Random 1

418: Random 2

Figure 33

A	B	C	D	E	F	G
---	---	---	---	---	---	---

A: Message type (REQuest or AUTHorization; REQuest in this case)

B: Success Code for response to this message

C: Failure Code for response to this message

D: DID of message sending device

E: DID of other transacting party's device

F: Transaction amount or some other agreed transaction description

G: Friendly name of account to be used to pay D's user, amount E

F is optional and might be specified in AUTHorization message

Figure 34

A	B	C	D	E	F
---	---	---	---	---	---

A: Message type (REQuest or AUTHorization; REQuest in this case)

B: Success Code for response to this message

C: Failure Code for response to this message

D: DID of message sending device

E: DID of other transacting party's device

F: Transaction amount or some other agreed transaction description

A	B	C
---	---	---

A: The Success or Failure code indicated by Payer depending on whether the REQuest was successful or not

B: A randomly generated number to be used to refer to the transaction for the remainder of the change

C: Payer's account listing

A	B
---	---

A: The Success or Failure code indicated by Payer depending on whether the REQest was successful or not

B: A randomly generated number to be used to refer to the transaction for the remainder of the exchange

A	B	C	D	E
---	---	---	---	---

A: Message type (REQUEST or AUTHORIZATION; AUTHORIZATION in this case)

B: Success Code for response to this message

C: Failure Code for response to this message

D: A reference to the transaction been authorized; a previously STS-generated reference is used

E: Optional to reference payer's account if not previously specified

A	B	C	D	E
---	---	---	---	---

A: Message type (REQuest or AUTHorization; AUTHorization in this case)

B: Success Code for response to this message

C: Failure Code for response to this message

D: A reference to the transaction been authorized; a previously STS-generated reference is used

E: Optional to reference payee's account if not previously specified

Figure 39

A	B
---	---

A: The Success or Failure code indicated by Payer depending on whether the Authorization was successful or not

B: An optional additional description, for example a service token value (receipt)

A	B
---	---

A: The Success or Failure code indicated by Payee depending on whether the Authorization was successful or not

B: An optional additional description, for example a service token value (receipt)

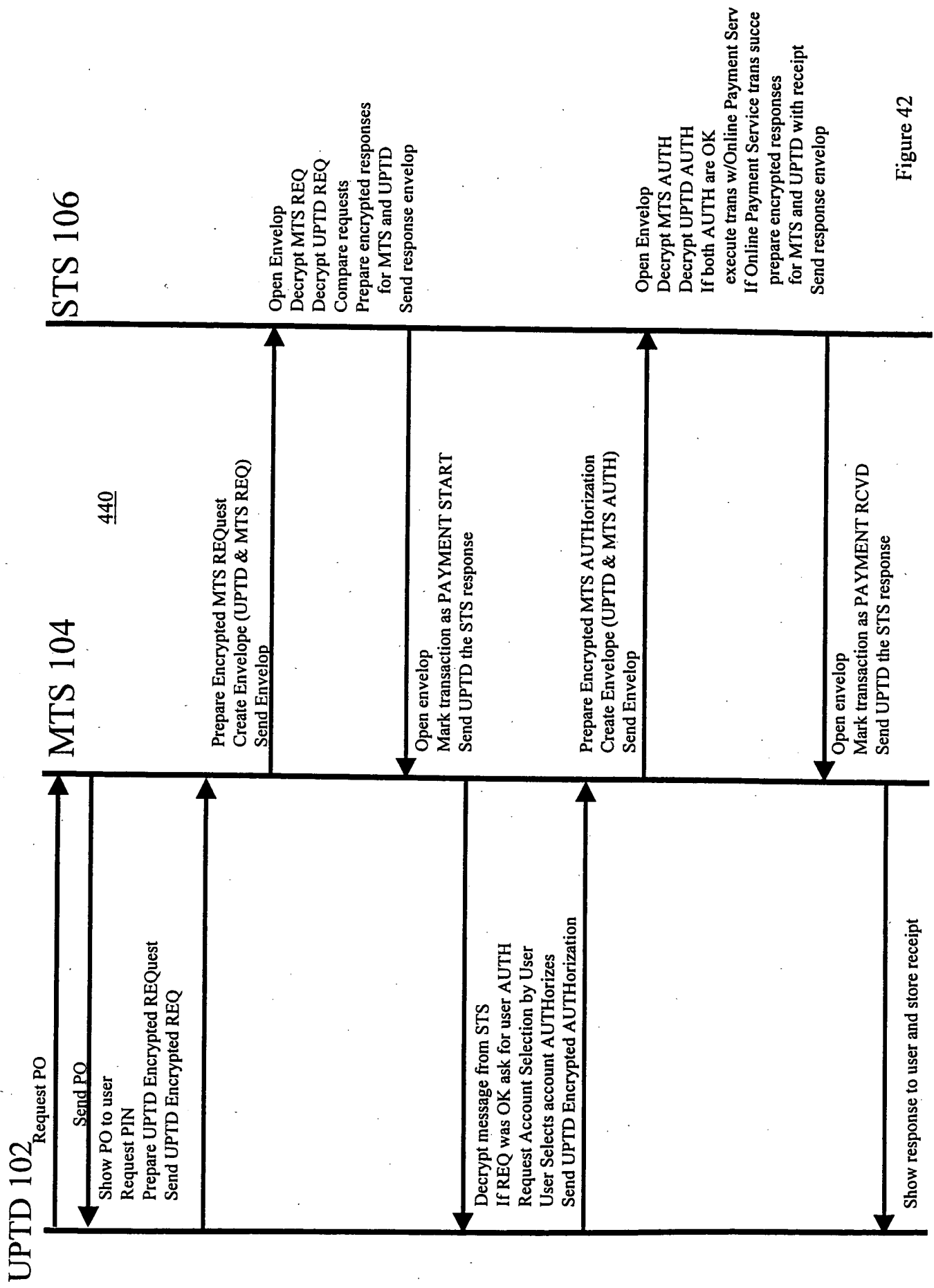


Figure 42

1 Consumer Requests Purchase Order (PO)

2 Consumer Receives PO

3 Consumer REQUESTS transaction (consumer enters PIN)

4 MTS sends MTS REQ and consumer REQ

5 STS requests from Online Payment Service the account listing for consumer

6 STS receives Online Payment Service account listing

7 STS Sends response to REQ with accounts for consumer

8 MTS forwards STS response to REQ to consumer

9 Consumer AUTHORIZES transaction (consumer selects account)

10 MTS sends MTS AUTH and consumer AUTH

11 STS sends transaction to Online Payment Service

12 STS receives Online Payment Service response

13 STS sends response to AUTH

14 MTS forward STS response to AUTH to consumer

(consumer sees notification of success on his display)

Laptop
Windows XP
.NET Framework
WLAN AP (directly connected)
Web server, DHCP server
.NET Web application (store)
Web service interface for STS comm.

Merchant
Transaction
Server 104

Online
Payment
Service 108

Desktop Server
Windows XP

.NET application
Web service interface

for MTS comm.

Secure
Transaction
Server 106

For each Device ID

• Random Seed

• PIN

• Online Payment Service account
and password

PDA

StrongArm w/PocketPC

Compact .NET

client application

WLAN CF

102

Figure 43

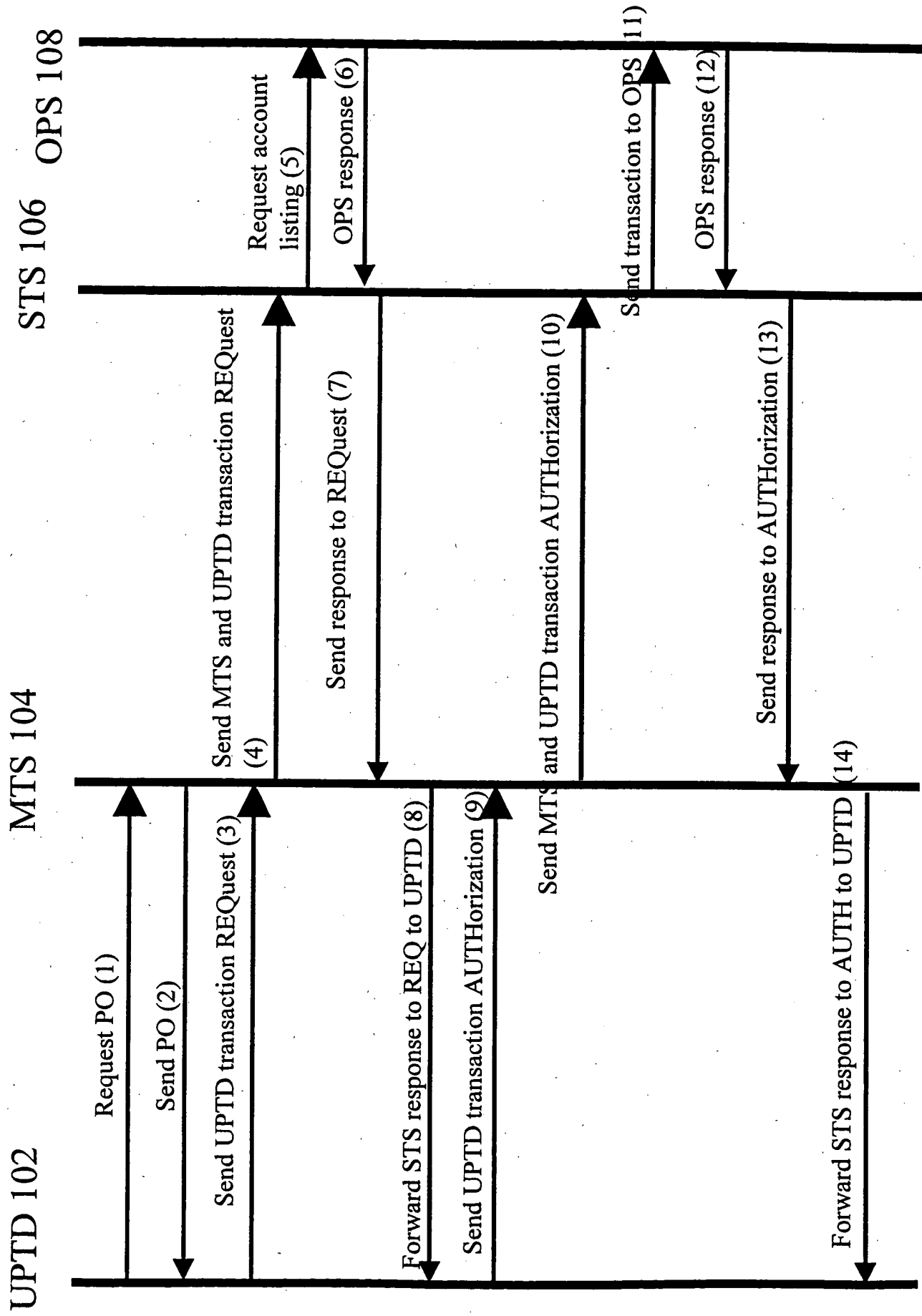


Figure 44

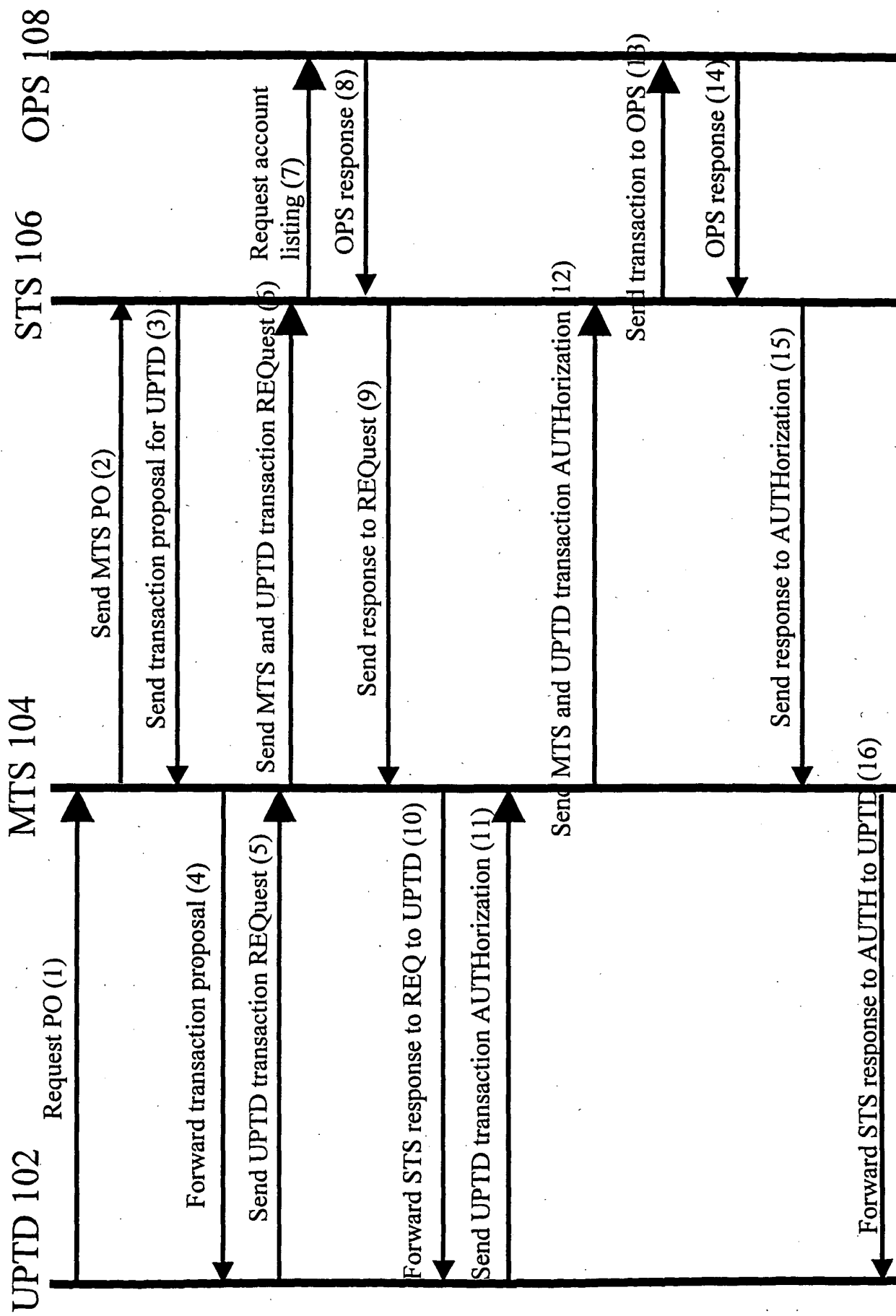
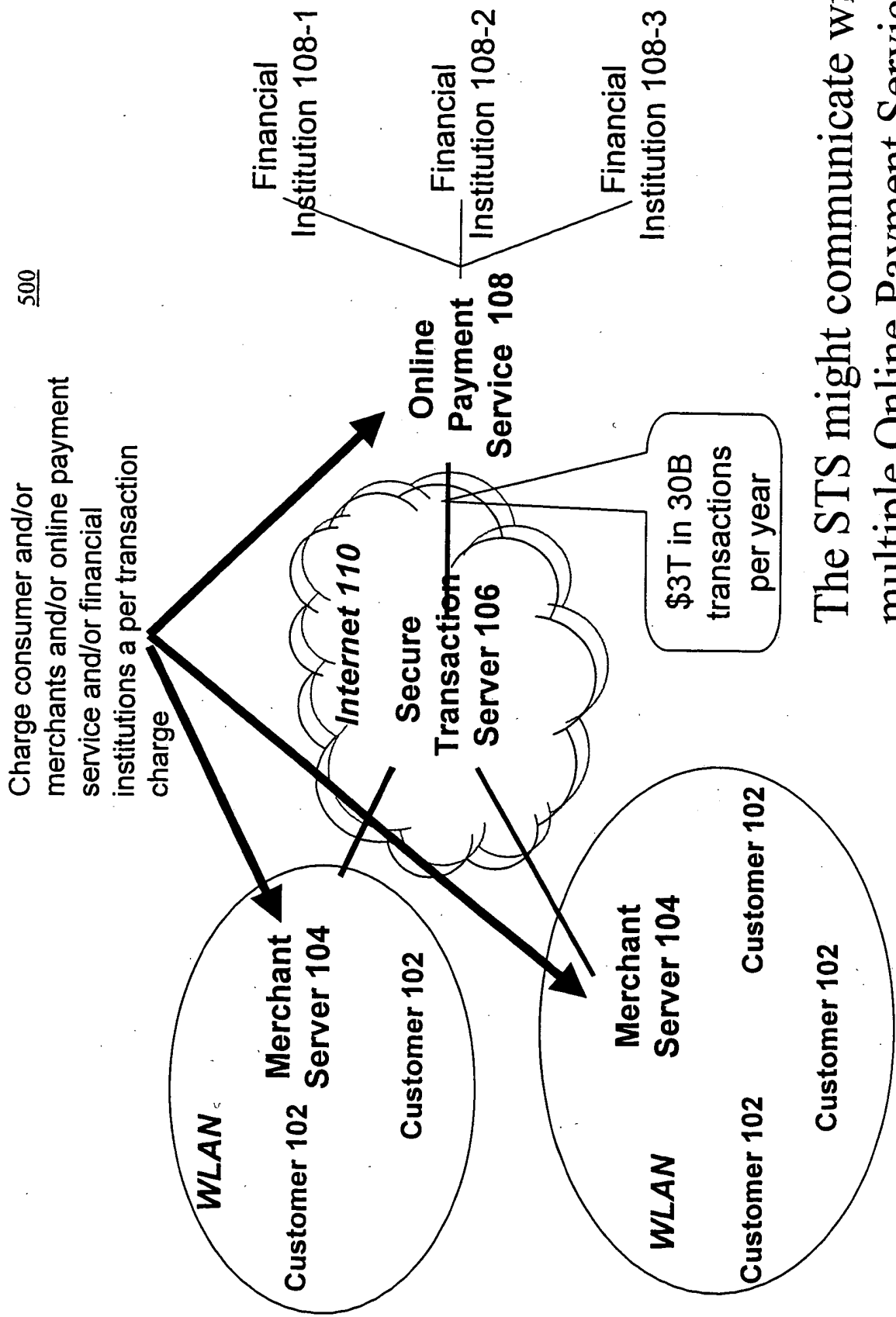


Figure 45



The STS might communicate with multiple Online Payment Services

Figure 46

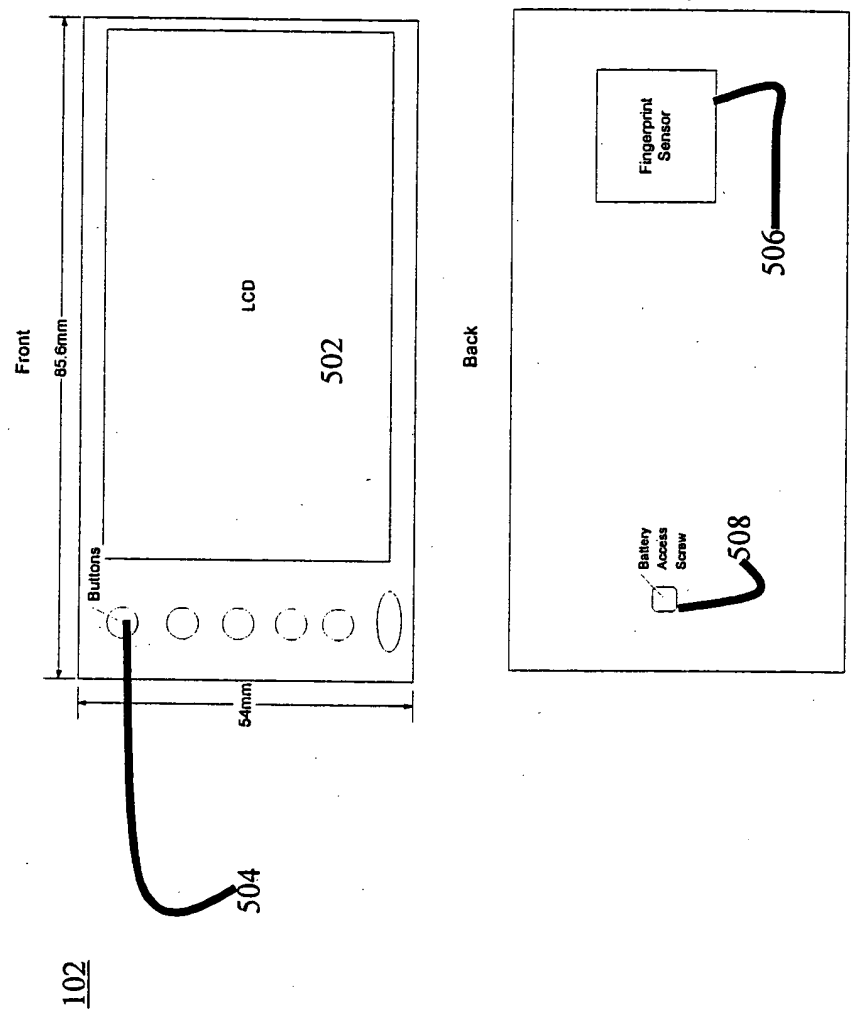


Figure 47

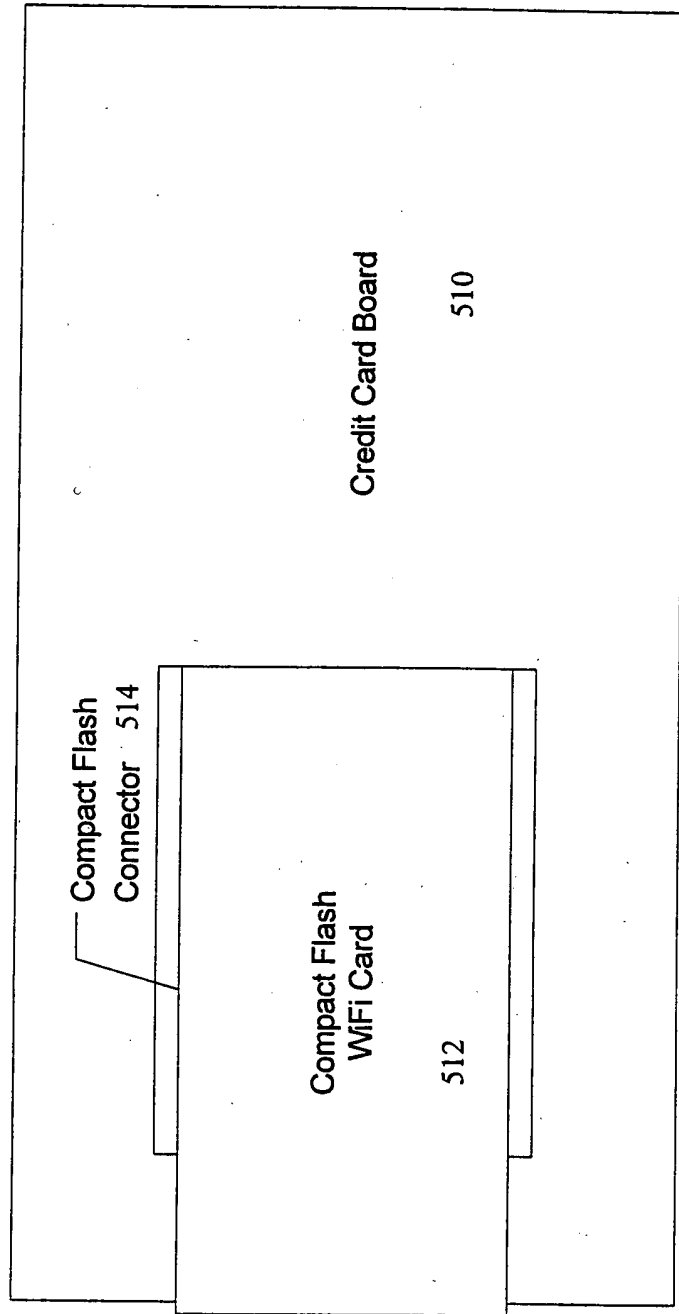


Figure 48

Side View (not to scale) 102

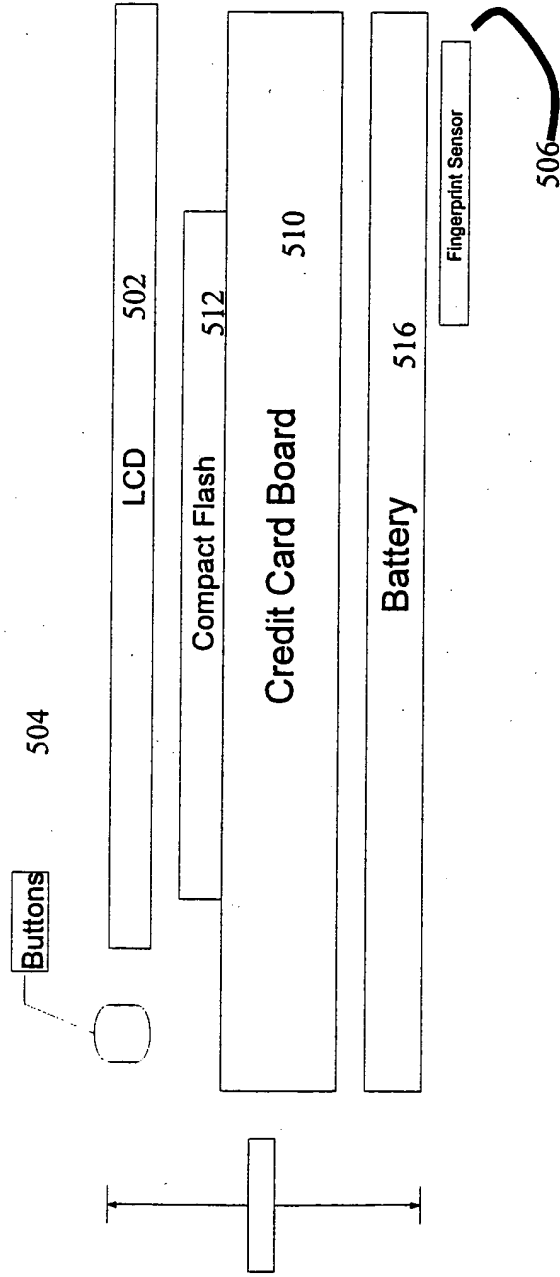


Figure 49

Side View (not to scale)

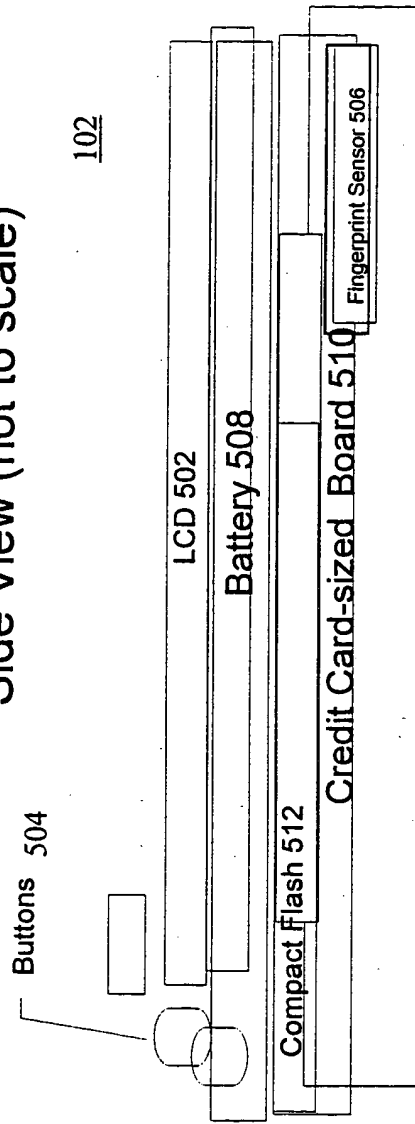


Figure 50

Pre-purchasing phase, example 600

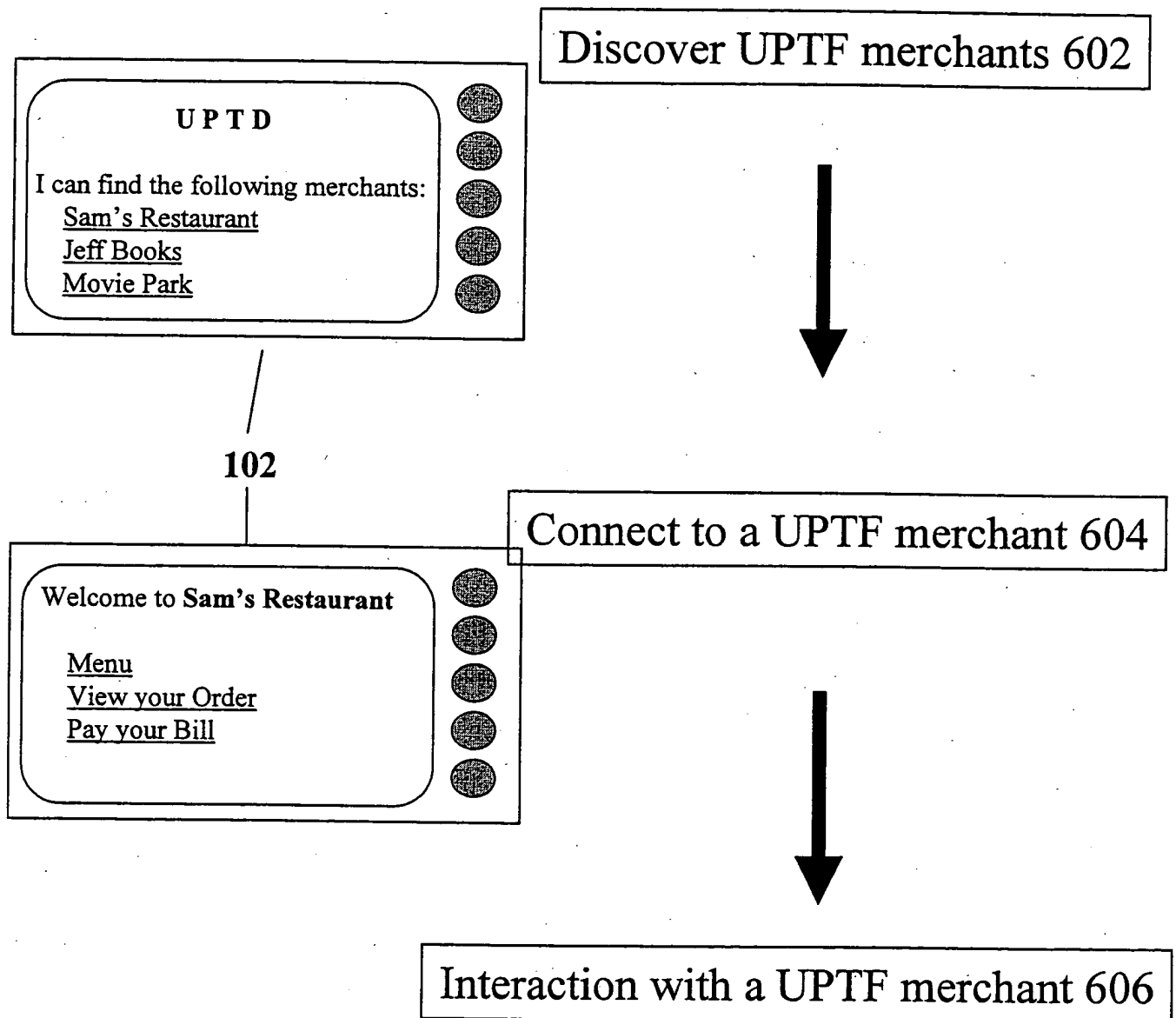


Figure 51

Physical Goods

Purchase I, example 610

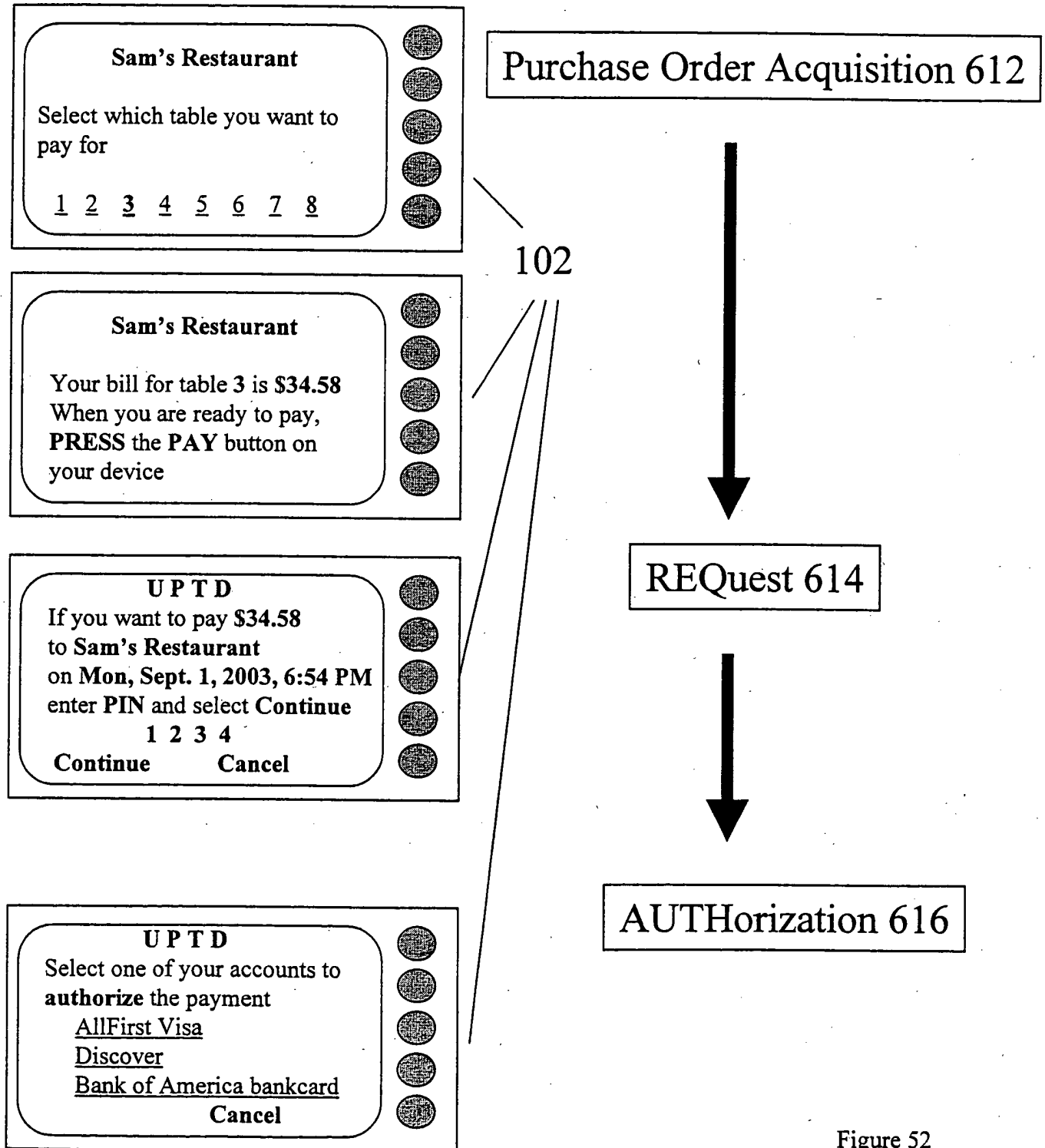


Figure 52

Physical Goods Purchase I, example, variation 620

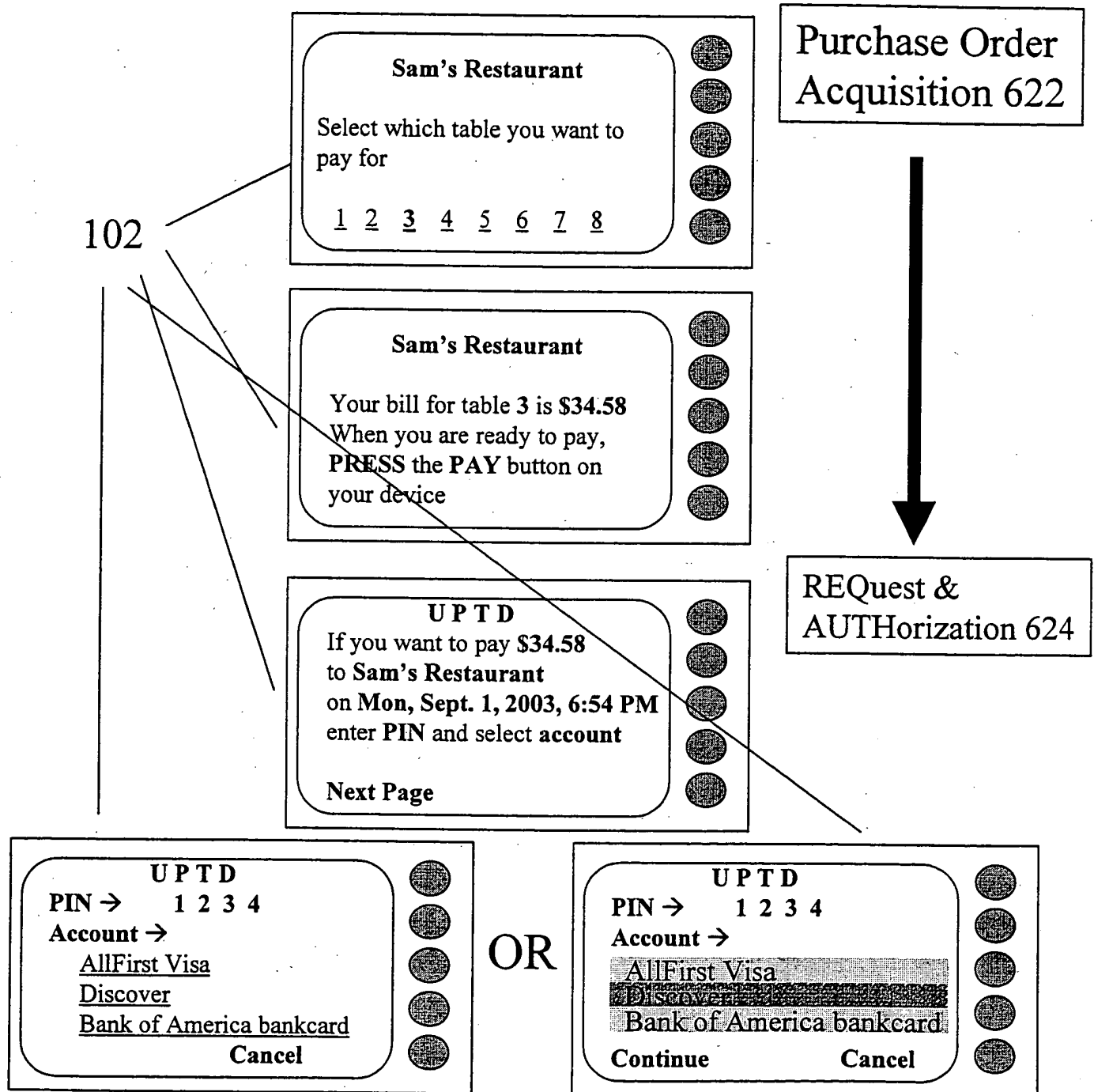


Figure 53

Physical Goods Purchase II, example 630

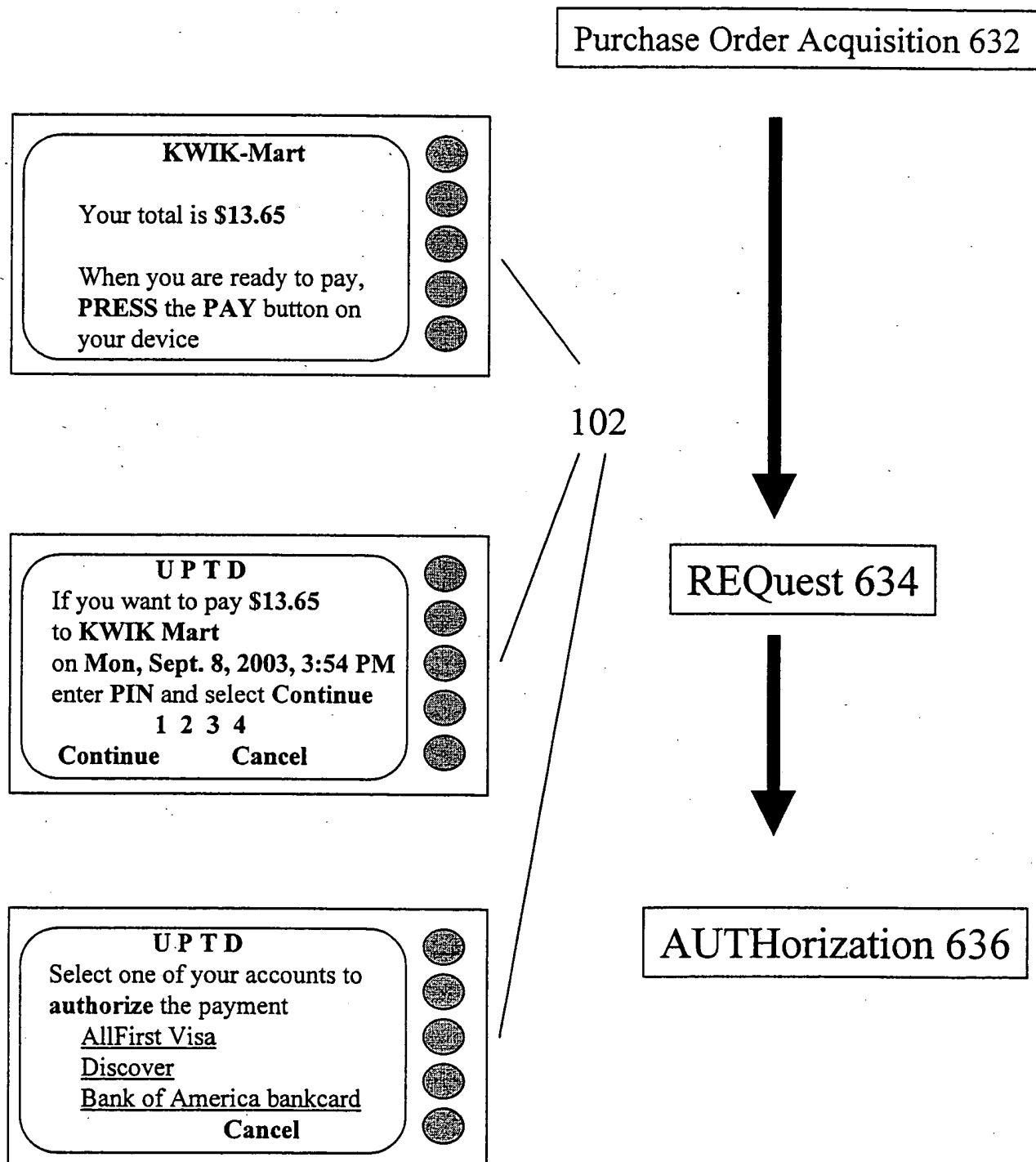


Figure 54

Service Purchase I, example 638

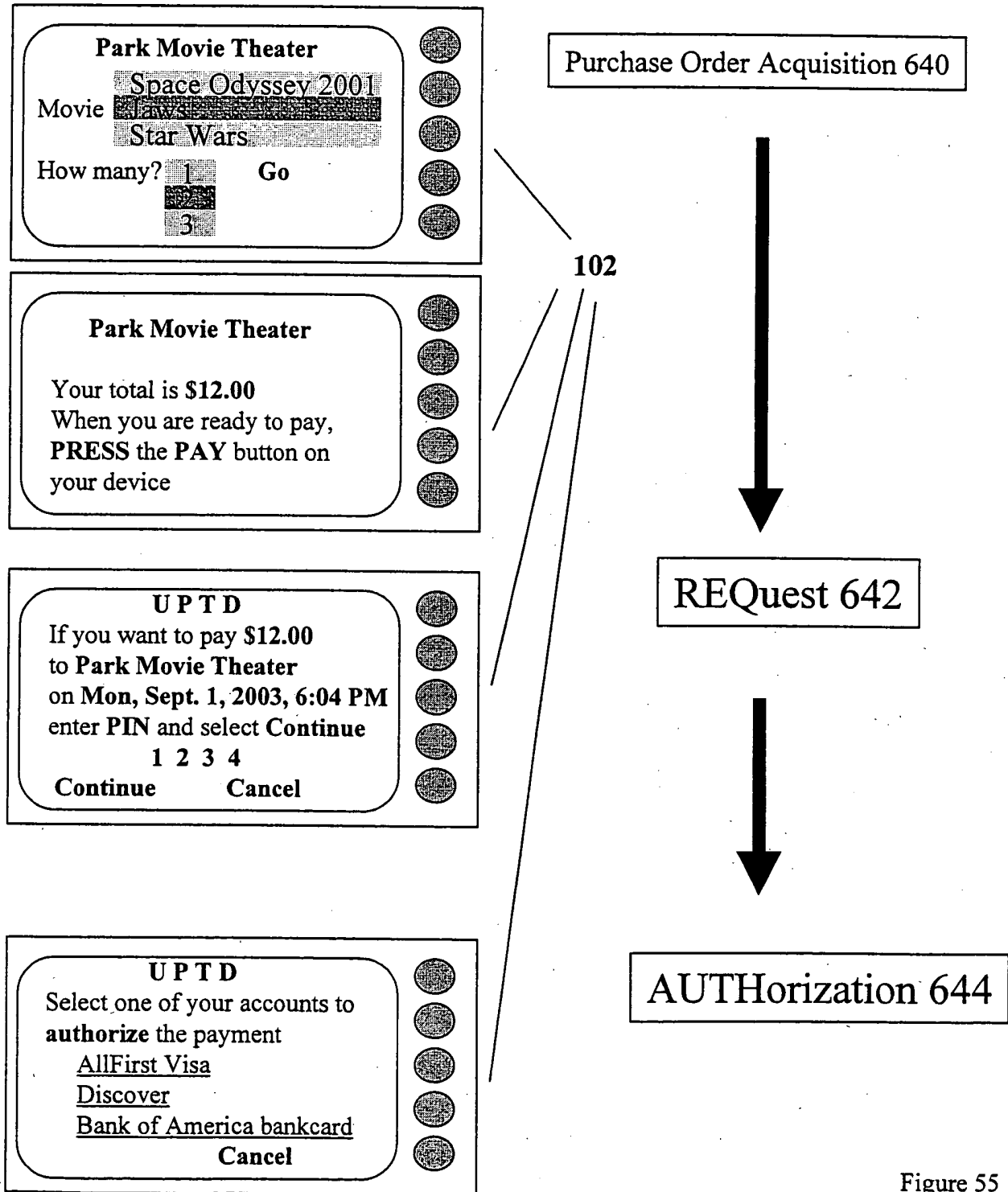


Figure 55

Service Purchase I – token verification and consumption, example 650

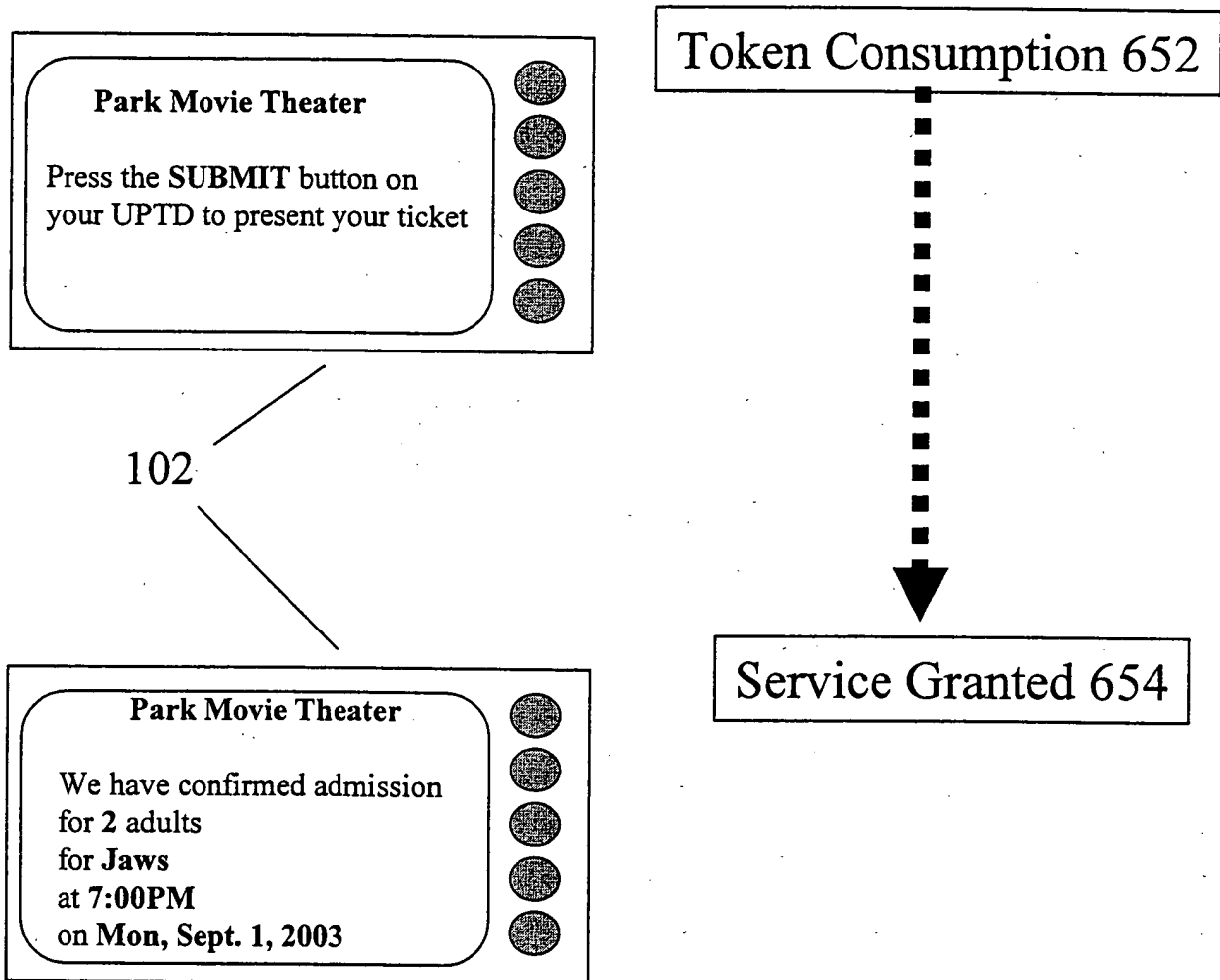


Figure 56

1100

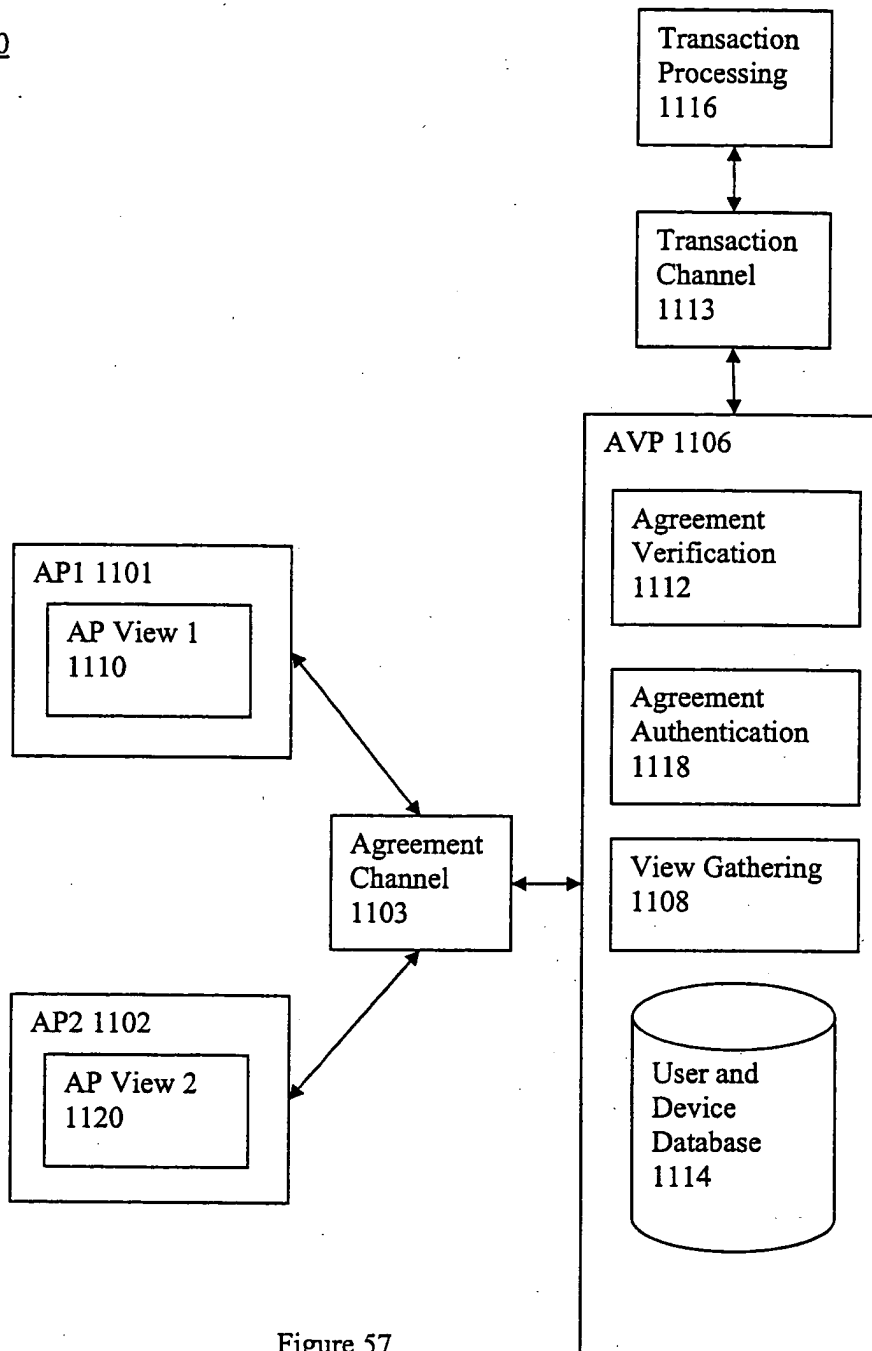


Figure 57

1200

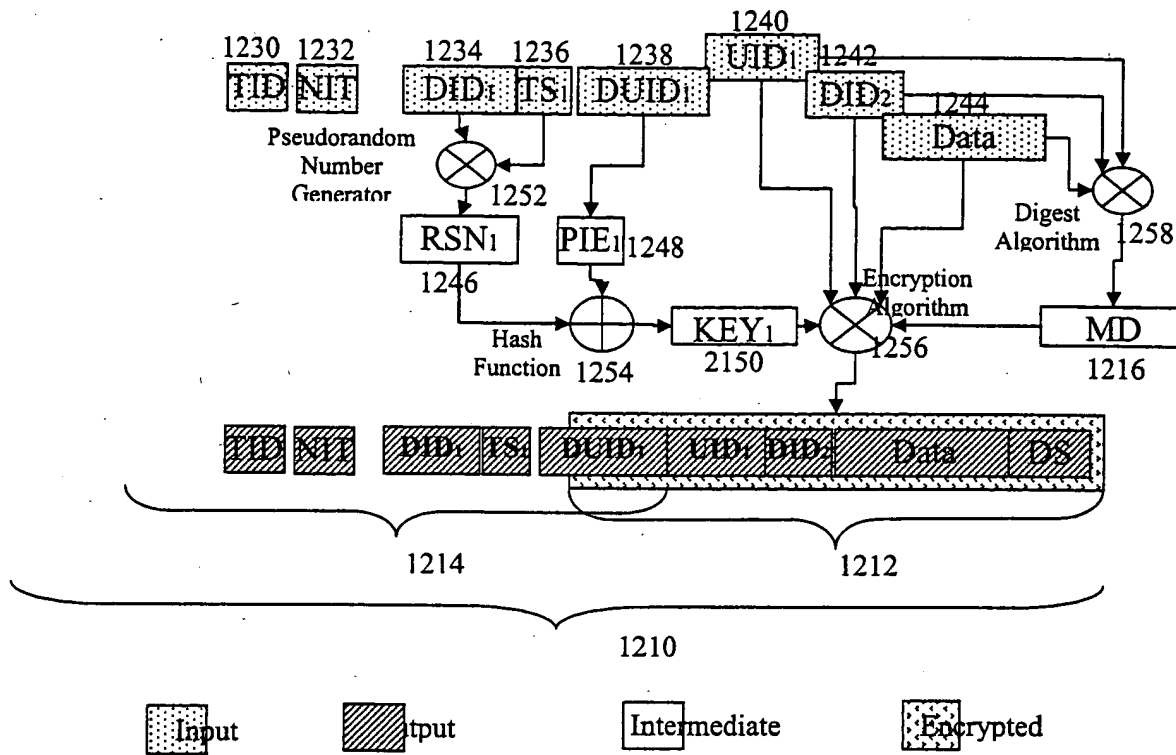


Figure 58

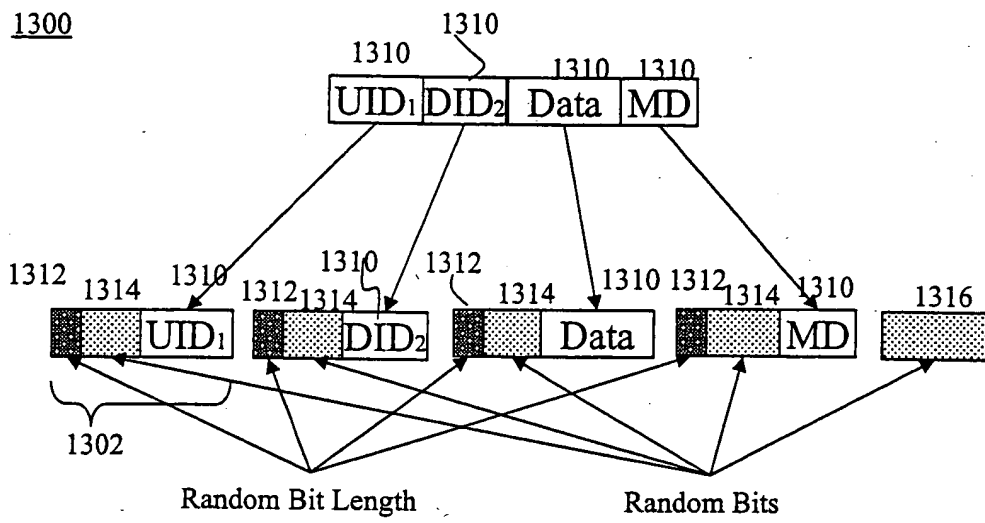


Figure 59

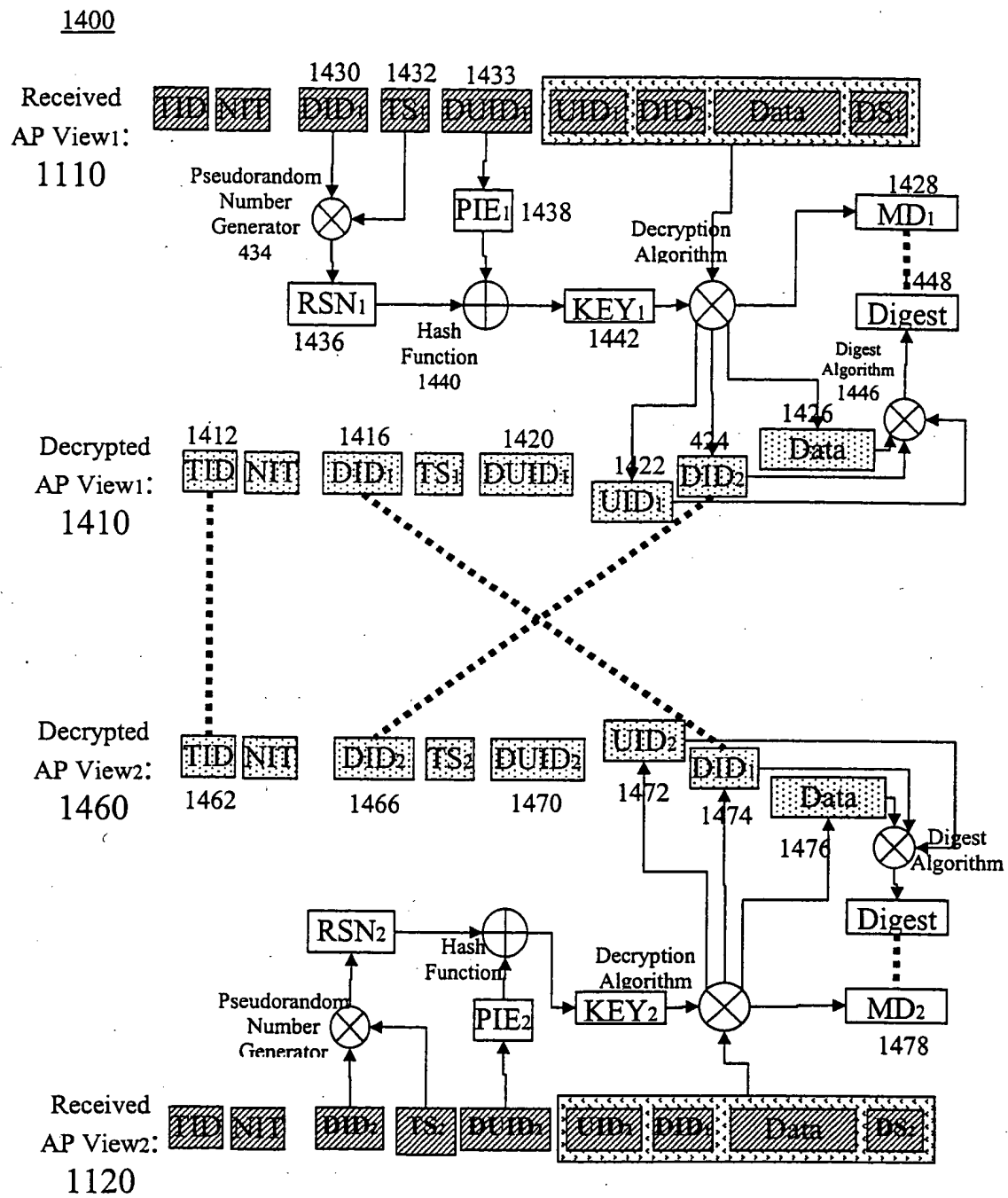


Figure 60

1500

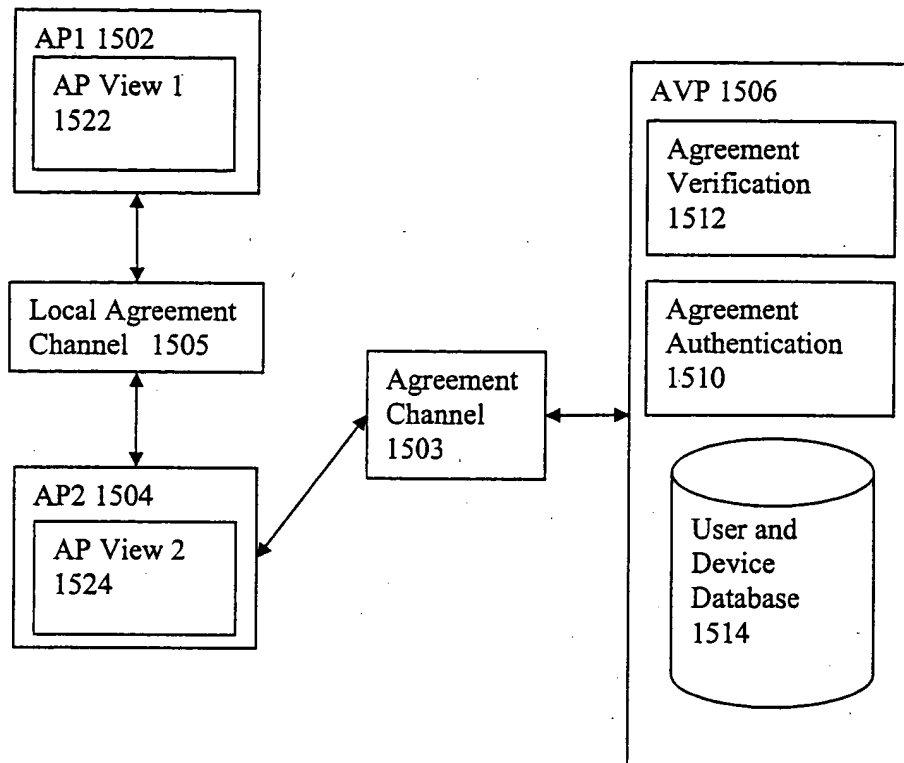


Figure 61

1600

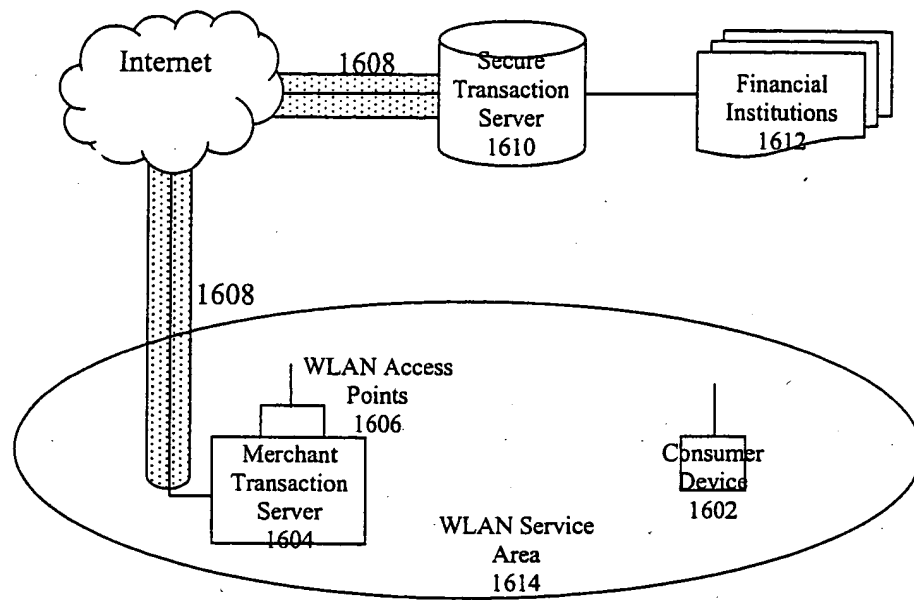


Figure 62

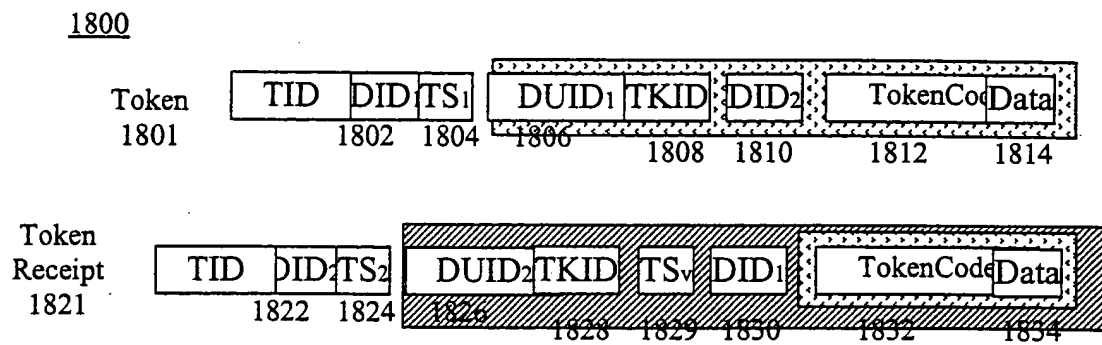


Figure 63